PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 May 2001 (02.05.01)	
International application No. PCT/JP00/05832	**Applicant's or agent's file reference** 900392
International filing date (day/month/year) 29 August 2000 (29.08.00)	**Priority date** (day/month/year) 30 August 1999 (30.08.99)
Applicant HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

26 March 2001 (26.03.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Kiwa Mpay
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Copy for the Elected Office (EO/US) PCT/JP00/05832

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

FUKAMI, Hisao
Mitsui Sumitomo Bank
Minamimorimachi Bldg.
1-29, Minamimorimachi 2-chome,
Kita-ku
Osaka-shi, Osaka 530-0054
JAPON

Date of mailing (day/month/year)
17 July 2001 (17.07.01)

Applicant's or agent's file reference
900392

IMPORTANT NOTIFICATION

International application No.
PCT/JP00/05832

International filing date (day/month/year)
29 August 2000 (29.08.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address
1) FUKAMI, Hisao
2) MORITA, Toshio
3) HORII, Yutaka
Sumitomo Bank Minamimori-machi Building
1-29, Minamimori-machi 2-chome
Kita-ku, Osaka-shi
Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.: 06-6361-2021
Facsimile No.: 06-6361-1731
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
1) FUKAMI, Hisao
2) MORITA, Toshio
3) HORII, Yutaka
Mitsui Sumitomo Bank Minamimorimachi Bldg.
1-29, Minamimorimachi 2-chome,
Kita-ku, Osaka-shi, Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.: 06-6361-2021
Facsimile No.: 06-6361-1731
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[X] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorized officer
Shinji IGARASHI
Telephone No.: (41-22) 338.83.38

特許協力条約に基づく国際出願願書
副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

SK01PCT87

0 0-1	受理官庁記入欄 国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	

PCT
21.6.01
受領印

0-4 0-4-1	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、 右記によって作成された。	 PCT-EASY Version 2.91 (updated 01.01.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	SK01PCT87
I	発明の名称	情報処理装置及び処理方法
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号
II-5en	Address:	7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	浅野 智之
III-1-4en	Name (LAST, First)	ASANO, Tomoyuki
III-1-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-1-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP

特許協力条約に基づく国際出願願書 SK01PCT87
副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

III-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-2-2	右の指定国についての出願人である。	米国のみ (US only)
III-2-4ja	氏名(姓名)	大澤 義知
III-2-4en	Name (LAST, First)	OSAWA, Yoshitomo
III-2-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍 (国名)	日本国 JP
III-2-7	住所 (国名)	日本国 JP
III-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-3-2	右の指定国についての出願人である。	米国のみ (US only)
III-3-4ja	氏名(姓名)	石黒 隆二
III-3-4en	Name (LAST, First)	ISHIGURO, Ryuji
III-3-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-3-6	国籍 (国名)	日本国 JP
III-3-7	住所 (国名)	日本国 JP
III-4	その他の出願人又は発明者	
III-4-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-4-2	右の指定国についての出願人である。	米国のみ (US only)
III-4-4ja	氏名(姓名)	光澤 敦
III-4-4en	Name (LAST, First)	MITSUZAWA, Atsushi
III-4-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-4-6	国籍 (国名)	日本国 JP
III-4-7	住所 (国名)	日本国 JP

特許協力条約に基づく国際出願願書 SK01PCT87
副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

III-5	その他の出願人又は発明者	
III-5-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-5-2	右の指定国についての出願人である。	米国のみ (US only)
III-5-4ja	氏名(姓名)	大石 丈於
III-5-4en	Name (LAST, First)	OISHI, Tateo
III-5-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-5-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-5-6	国籍 (国名)	日本国 JP
III-5-7	住所 (国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	小池 晃
IV-1-1en	Name (LAST, First)	KOIKE, Akira
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門二丁目６番４号　第１１森ビル
IV-1-2en	Address:	No.11 Mori Bldg., 6-4, Toranomon 2-chome, Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3508-8266
IV-1-4	ファクシミリ番号	03-3508-0439
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	田村 榮一; 伊賀 誠司
IV-2-1en	Name(s)	TAMURA, Eiichi; IGA, Seiji
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国である他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国である他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR 及びヨーロッパ特許条約と特許協力条約の締約国である他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締約国である他の国
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

特許協力条約に基づく国際出願願書 SK01PCT87
副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

V-3	国内特許(この版の EASY の配布後に特許協力条約の締約国になった国)	CO コロンビア EC エクアドル	
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。		
V-6	指定の確認から除かれる国	なし (NONE)	
VI-1	先の国内出願に基づく優先権主張		
VI-1-1	先の出願日	2000年06月21日 (21.06.2000)	
VI-1-2	先の出願番号	特願2000-186172	
VI-1-3	国名	日本国 JP	
VI-2	先の国内出願に基づく優先権主張		
VI-2-1	先の出願日	2000年06月21日 (21.06.2000)	
VI-2-2	先の出願番号	特願2000-186173	
VI-2-3	国名	日本国 JP	
VI-3	先の国内出願に基づく優先権主張		
VI-3-1	先の出願日	2000年08月10日 (10.08.2000)	
VI-3-2	先の出願番号	特願2000-243204	
VI-3-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	5	-
VIII-2	明細書	52	-
VIII-3	請求の範囲	9	-
VIII-4	要約	1	absk01pct87.txt
VIII-5	図面	29	-
VIII-7	合計	96	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-10	包括委任状の写し	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1, VI-2, VI-3	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-18	要約書とともに提示する図の番号	12	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	小池 晃	

特許協力条約に基づく国際出願願書 SK01PCT87
副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

IX-2	提出者の記名押印	
IX-2-1	氏名(姓名)	田村 榮一
IX-3	提出者の記名押印	
IX-3-1	氏名(姓名)	伊賀 誠司

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2 10-2-1 10-2-2	図面 : 受理された 不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日 (訂正日)	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

PCT手数料計算用紙(願書付属書)　SK01PCT87

副本 - 印刷日時 2001年06月21日 (21.06.2001) 木曜日 15時08分13秒

[この用紙は、国際出願の一部を構成せず、国際出願の用紙の枚数に算入しない]

0 0-1	受理官庁記入欄 国際出願番号.			
0-2	受理官庁の日付印			
0-4 0-4-1	様式-PCT/RO/101 (付属書) このPCT手数料計算用紙は、 右記によって作成された。	PCT-EASY Version 2.91 (updated 01.01.2001)		
0-9	出願人又は代理人の書類記号	SK01PCT87		
2	出願人	ソニー株式会社		
12	所定の手数料の計算	金額/係数	小計 (JPY)	
12-1	送付手数料 T	⇨	18,000	
12-2	調査手数料 S	⇨	72,000	
12-3	国際手数料 基本手数料 (最初の30枚まで) b1	46,200		
12-4	30枚を越える用紙の枚数	66		
12-5	用紙1枚の手数料 (X)	1,100		
12-6	合計の手数料 b2	72,600		
12-7	b1 + b2 = B	118,800		
12-8	指定手数料 国際出願に含まれる指定国数	88		
12-9	Number of designation fees payable (maximum 6)	6		
12-10	1指定当たりの手数料 (X)	10,000		
12-11	合計の指定手数料 D	60,000		
12-12	PCT-EASYによる料金の減額 R	-14,000		
12-13	国際手数料の合計 (B+D-R) I	⇨	164,800	
12-17	納付するべき手数料の合計 (T+S+I+P)	⇨	254,800	
12-19	支払方法	送付手数料: 特許印紙 調査手数料: 特許印紙 国際手数料: 銀行口座への振込み 優先権証明書請求手数料: 特許印紙		

EASYによるチェック結果と出願人による言及

13-1-1	出願人による言及 注釈	６７７３　弁理士　小池　晃 ８６３３　弁理士　田村　榮一 ９６６７　弁理士　伊賀　誠司
13-2-2	EASYによるチェック結果 指定国	Green? より多くの指定が可能です。(以下の国が指定からはずされています:　JP) 確認してください。
		Yellow! "追加する指定国"の欄を用いた指定がなされていますが、この欄を用いることなく、更新された最新のメインテナンステーブルを入手し使用することを推奨します。

(12)特許協力条約に基づいて公開された国際...

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年12月27日 (27.12.2001)

PCT

(10) 国際公開番号
WO 01/99333 A1

(51) 国際特許分類[7]: H04L 9/00, G11B 20/10, G10K 15/02, G06F 12/14

(21) 国際出願番号: PCT/JP01/05327

(22) 国際出願日: 2001年6月21日 (21.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-186172 2000年6月21日 (21.06.2000) JP
特願2000-186173 2000年6月21日 (21.06.2000) JP
特願2000-243204 2000年8月10日 (10.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]. 大石丈於 (OISHI, Tateo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

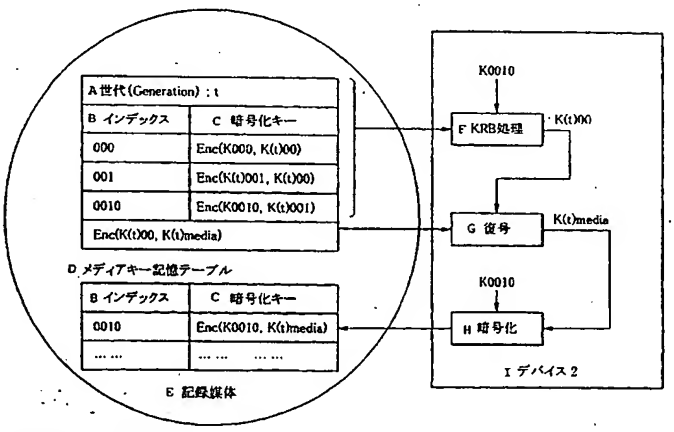
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND PROCESSING METHOD

(54) 発明の名称: 情報処理装置及び処理方法



A...GENERATION (Generation):t
B...INDEX
C...ENCRYPTING KEY
D...MEDIA KEY STORING TABLE
E...RECORDING MEDIUM
F...KRB PROCESSING
G...DECODING
H...ENCRYPTING
I...DEVICE 2

(57) Abstract: An information recording/reproducing device for executing a key distribution by a KRB distribution involving a tree-structure key distribution configuration. The device transmits, by using a key-structure key distribution configuration, a key such as a master key, a media key or a content key along with a key update block (KRB). The recording/reproducing device, after calculating and acquiring the key of a certain recording medium based on a reception KRB, encrypts the acquired key using an encryption key specific to the device, for example, a leaf key, and stores it in a recording medium or memory of the device. Therefore, the recording/reproducing device can calculate a key by merely decoding the encrypting key one time when next using the recording medium or contents, and can reduce computational complexity such as KRB decoding required when the device accesses a recording medium or uses contents, thereby making efficient processing on the KRB receiving side.

[続葉有]

WO 01/99333 A1

(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書

(57) 要約:

ツリー（木）構造の鍵配布構成としてのＫＲＢ配信によりキーの配布を実行する情報記録再生装置である。この装置は、ツリー構造の鍵配布構成により、マスターキー、メディアキー若しくはコンテンツキー等の鍵をキー更新ブロック（ＫＲＢ）とともに送信する。記録再生装置が受信ＫＲＢに基づき、ある記録媒体の鍵を計算して取得した後に、取得した鍵を、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する構成とした。従って、記録再生装置が、次にその記録媒体若しくはコンテンツを使用する際に、その暗号化キーを１回復号するだけで鍵を計算でき、記録再生装置が記録媒体にアクセス若しくはコンテンツを利用する際に必要となるＫＲＢ復号処理等の計算量を減少させることが可能となり、ＫＲＢ受信側での処理が効率化される。

明細書

情報処理装置及び処理方法

技術分野

本発明は、情報処理装置及び処理方法、情報記録媒体、並びにコンピュータ・プログラムに関し、特に、ツリー（木）構造の階層的鍵配信方式を用いてコンテンツデータの記録若しくは再生に必要な鍵、例えば、マスターキー、メディアキー若しくはコンテンツキー等を配信若しくは取得し、これを用いて各装置がコンテンツデータの記録若しくは再生を行う構成とした情報処理装置及び処理方法、情報記録媒体、並びにコンピュータ・プログラムに関する。

背景技術

ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、

再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、又はコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画

像や音声を再生することができる。

一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、正当なライセンスを受けている装置のみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）とにより暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな

記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

上記問題を解決する構成として、本出願人は、各情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な鍵（マスターキー若しくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキー若しくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願２０００－１０５３２８）している。具体的には、記録媒体への記録若しくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばｎ分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、

更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含むキー更新ブロック（ＫＲＢ：Key Renewal Block）を各情報記録再生装置に配信し、キー更新ブロック（ＫＲＢ）を受信した各情報記録再生装置のＫＲＢ復号処理により、各装置が記録若しくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

上述のような情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用いた場合、例えば記録媒体ごとに割り当てられるメディアキーをキー更新ブロック（ＫＲＢ）で暗号化して配信した場合、各情報記録再生装置は、各記録媒体にアクセスするたびに、すなわち、記録媒体が記録再生装置に装着されるたびに、キー更新ブロック（ＫＲＢ）及びデバイスキーを用いたメディアキーの計算を行わなければならない。この計算は、個々の暗号文の復号に要する時間と、メディアキーを暗号化するノードキーから記録再生装置が存在する葉までの木の深さの積に比例するため、装置数が多い、大きな記録システムにおいてはこの処理のオーバーヘッドが大きくなるという問題がある。

また、本出願人は、各情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な暗号鍵としてのコンテンツキーを提供する構成を先に提案し、すでに特許出願（特願２０００－１０５３２９）している。これは、例えば通信回線を介して、コンテンツデータと、コンテンツデータを暗号化しているコンテンツキーを併せて送付するものであり、コンテンツキーは暗号化データとして送付する構成である。

暗号化コンテンツキーの提供は、例えばｎ分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理したキー更新ブロック（ＫＲＢ）を用いて行われ、更新ノードキーでコンテンツキーを暗号化して提供することにより、正当な記録再生装置のみがコンテンツキーを取得可能としている。

上述のような情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用いて暗号化コンテンツキーを提供する場合、各情報記録再生装置は、

コンテンツを利用するたびに、例えば、記録媒体からコンテンツを再生するたびに、ＫＲＢをデバイスキー（リーフキー）を用いて処理し、コンテンツキーの計算を行わなければならない。

この計算は、個々の暗号文の復号に要する時間と、コンテンツキーを暗号化するノードキーからデータ処理装置が存在する葉までの木の深さの積に比例するため、装置数が多い、大きなシステムにおいてはこの処理のオーバーヘッドが大きくなるという問題がある。

発明の開示

本発明は、上述の問題を解決するものであり、情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用いた構成において、キー更新ブロック（ＫＲＢ）に基づく暗号化キー又は復号キーの算出処理を省略し、短時間で必要な暗号化キー又は復号キーを取得可能とした構成を提供することを目的とする。具体的には、例えばある記録再生装置がある記録媒体のメディアキーを計算により取得した後に、その取得したメディアキーを、その記録再生装置に固有の暗号鍵を用いて暗号化して格納しておき、次にその記録媒体を使用する際に、その暗号文を１回復号するだけでメディアキーを計算できる構成として、短時間で必要な暗号化キー又は復号キーを取得可能とした情報処理装置、情報処理方法、及び情報記録媒体、並びにコンピュータ・プログラムを提供することを目的とする。

また、本発明は、情報記録再生装置をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用いたコンテンツキーの提供構成において、キー更新ブロック（ＫＲＢ）に基づく暗号化キー又は復号キーの算出処理を省略し、短時間で必要な暗号化キー又は復号キーとしてのコンテンツキーを取得可能とした構成を提供することを目的とする。具体的には、例えばある記録再生装置がある記録媒体に格納されたコンテンツのコンテンツキーを計算により取得した後に、その取得したコンテンツキーを、その記録再生装置に固有の暗号鍵を用いて暗号化して格納しておき、次にそのコンテンツを再生する際に、その暗号文を１回復号するだけ

でコンテンツキーを計算できる構成として、短時間で必要な暗号化キー又は復号キーとしてのコンテンツキーを取得可能とした情報処理装置、情報処理方法、及び情報記録媒体、並びにコンピュータ・プログラムを提供することを目的とする。

本発明は、暗号化されたデータを処理する情報処理装置であり、この装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理装置内の記憶領域に格納する。

また、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納する。

さらに、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、暗号化処理を実行する暗号処理手段を有し、暗号処理手段は、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、算出した

復号用キーを、復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて情報処理装置内の記憶領域に格納する。

さらにまた、本発明に係る暗号化されたデータを処理する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、復号処理を実行する復号処理手段を有し、復号処理手段は、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、復号用キーが検出された場合には、記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、復号用キーが検出されなかった場合には、記憶手段に保有したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する。

本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、この算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納する。

また、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、暗号化されたデータを復号処理する際に用い

られる復号用キーの算出処理を実行し、この算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納する。

さらに、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、この算出した復号用キーを、復号用キーを用いて復号されるデータを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納する。

さらにまた、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法であり、この方法は、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、復号用キーが検出された場合には、記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、復号用キーが検出されなかった場合には、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する。

本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用い

られる復号用キーの算出処理を実行するステプと、算出した復号用キーに対して、情報処理装置固有のキーを用いた暗号化処理を行うステップと、暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納するステップとを具備する。

また、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、算出した復号用キーを、復号用キーの更新情報としての世代番号と対応付けて情報処理装置内の記憶領域に格納するステップとを具備する。

さらに、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、算出した復号用キーを、復号用キーを用いて復号されるデータを識別するための識別情報と対応付けて情報処理装置内の記憶領域に格納するステップとを具備する。

さらにまた、本発明は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において実行されるコンピュータ・プログラムであり、このプログラムは、記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込むステップと、暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索するステップと、復号用キーが検出された場合には、記録媒体又は情報処理装置内の記憶領域

に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出するステップと、復号用キーが検出されなかった場合には、情報処理装置に保有されているノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップとを具備する。

そして、本発明は、記録された情報が情報処理装置によって読み出し可能なように構成された情報記録媒体であり、情報処理装置に固有のキーによって暗号化処理を施した、暗号化されたデータを復号するための復号用キーが、情報処理装置の識別情報と関連付けてキー格納テーブルとして記録されている。

本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な鍵（マスターキー、メディアキー若しくはコンテンツキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。ツリー構造の鍵配布構成により、例えばメディアキーの更新をキー更新ブロック（ＫＲＢ）とともに送信し、記録再生装置が受信ＫＲＢに基づき、ある記録媒体のメディアキーを計算して取得した後に、取得したメディアキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する。従って、記録再生装置が、次にその記録媒体を使用する際に、その暗号化キーを１回復号するだけでメディアキーを計算でき、記録再生装置が記録媒体にアクセスする際に必要となるＫＲＢ復号処理等の計算量を減少させることが可能となる。

同様に、例えばツリー構造の鍵配布構成により、コンテンツ暗号処理用のコンテンツキーをキー更新ブロック（ＫＲＢ）とともに送信し、記録再生装置が受信ＫＲＢに基づきコンテンツキーを取得した後に、取得コンテンツキーをその記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する。従って、記録再生装置が、次にそのコンテ

ンツを再生利用する際に、その暗号化コンテンツキーを１回復号するだけでコンテンツキーを計算でき、記録再生装置がコンテンツ利用毎にＫＲＢ復号処理を実行する必要を排除できる。

なお、本発明のプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。

図面の簡単な説明

図１は、本発明の情報記録再生装置の構成例を示すブロック図である。

図２Ａ及び図２Ｂは、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図３Ａ及び図３Ｂは、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図４は、本発明の情報記録再生装置に対するメディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図５Ａ及び図５Ｂは、本発明の情報記録再生装置に対するメディアキー等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

図６は、情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲ

Ｂ）を使用した配布例と復号処理例を示す図である。

図７は、本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

図８は、本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

図９は、本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

図１０は、本発明の情報記録再生装置において適用可能なブロックキーの生成方法を説明する図である。

図１１は、本発明の情報記録再生装置におけるメディアキーを使用したデータ再生処理時の復号処理を説明するブロック図である。

図１２は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理例を示す図である。

図１３は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理フロー（例１）を示す図である。

図１４は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理フロー（例２）を示す図である。

図１５は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理例を示す図である。

図１６は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理フローを示す図である。

図１７は、本発明の情報記録再生装置の変形例におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理例を示す図である。

図１８は、本発明の情報記録再生装置に対するコンテンツキー等の鍵の暗号化処理について説明するツリー構成図である。

図１９Ａ及び図１９Ｂは、本発明の情報記録再生装置に対するコンテンツキー

等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

図２０は、本発明の情報記録再生装置に対するコンテンツ及びコンテンツキーの提供時のデータ構成例を示す図である。

図２１は、情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

図２２は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理例を示す図である。

図２３は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用したコンテンツ復号処理、キー格納処理フロー（例１）を示す図である。

図２４は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用したコンテンツ記録処理とキー格納処理フローを示す図である。

図２５は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用したコンテンツ復号処理、キー格納処理例を示す図である。

図２６は、本発明の情報記録再生装置におけるコンテンツキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理、キー格納処理フローを示す図である。

図２７Ａ及び図２７Ｂは、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図２８Ａ及び図２８Ｂは、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図２９は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

以下、本発明の具体的な構成を図面を参照して説明する。

図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック

図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ(Read Only Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５の記録媒体インタフェース（Ｉ／Ｆ）１９０を有し、これらはバス１１０によって相互に接続されている。

入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Circuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、又は復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行するこ

とで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。記録媒体インタフェース１９０は、ディジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。なお、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記憶する構成としてもよい。

モデム２００は、電話回線を介して外部の装置と接続する。例えば、インターネット・サービス・プロバイダ（ＩＳＰ：Internet Service Provider）のサーバと接続し、インターネット上のコンテンツ配信サーバなどとの通信路を確立する。

記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリなど、ディジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

次に、図１の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図２Ａ、図２Ｂ及び図３Ａ、図３Ｂのフローチャートを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図２Ａのフローチャートにしたがった記録処理が行われる。即ち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ２０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、暗号処理手段１５０に出力する。

暗号処理手段Ｉ５０は、ステップＳ２０２において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、記録媒体Ｉ／Ｆ１９０に出力する。暗号化コンテンツは、記録媒体Ｉ／Ｆ１９０を介して記録媒体１９５に記録（Ｓ２０３）され、記録処理

を終了する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ２０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。なお、ＤＴＣＰの規格書は、DTLA (Digital Transmission Licensing Administrator)からインフォメイショナルバージョン(Informational Version)を誰でも取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図２Ｂのフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ２２１において、そのアナログコンテンツを受信し、ステップＳ２２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ２２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段Ｉ５０に供給される。

以下、ステップＳ２２４、Ｓ２２５において、図２Ａのステップ２０２、Ｓ２０３における処理と同様の処理が行われる。すなわち、暗号処理手段Ｉ５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図３Ａ及び図３Ｂのフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図３Ａのフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップＳ３０１において、記録媒体Ｉ／Ｆ１９０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

暗号処理手段１５０では、ステップＳ３０２において、記録媒体Ｉ／Ｆ１９０から供給される暗号化コンテンツが復号処理され、復号データがバス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。ステップＳ３０３において、入出力Ｉ／Ｆ１２０はディジタルコンテンツを、外部に出力し、再生処理を終了する。

なお、入出力Ｉ／Ｆ１２０は、ステップＳ３０３で、IEEE1394シリアルバスを介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとし

て外部に出力する場合においては、図３Ｂのフローチャートに従った再生処理が行われる。

即ち、ステップＳ３２１、Ｓ３２２において、図３Ａのステップ３０１、Ｓ３０２における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段Ｉ５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

ＭＰＥＧコーデック１３０では、ステップＳ３２３において、ディジタルコンテンツがＭＰＥＧデコード、すなわち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ３２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換して、アナログコンテンツとする。そして、ステップＳ３２５に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

次に、図１に示した記録再生装置が、データを記録媒体に記録、若しくは記録媒体から再生する際に必要なキー、例えばマスターキー若しくはメディアキーを、各機器に配布する構成について説明する。ここで、マスターキーは、このシステムにおいて共通で、複数のデバイスにおいて共通に保持されるキーであり、デバイスの製造時にデバイス内に記録される。このキー配信システムを用いるデバイス全てにおいて共通であることが望ましい。また、メディアキーは、各記録媒体に固有のキーであり、記録媒体の製造時に記録媒体に記録される。理想的には全ての記録媒体毎に異なるキーであることが望ましいが、記録媒体の製造工程の制約上、複数の記録媒体を１グループとして、グループ毎に変えることが現実的である。例えば、記録媒体の製造ロットを１グループとして、ロット毎にメディアキーを変えるように構成してもよい。以下においては、これらのキーを更新する例を中心に述べるが、マスターキーが記録されていないデバイス若しくはメディアキーが記録されていない記録媒体に、それぞれのキーを配布及び記録するために本発明を用いることもできる。

図４は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図４の最下段に示すナンバ０～１５が個々の記録再生装置であ

る。すなわち図４に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーを自身に格納する。図４の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図４に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図４のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図４のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図４に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一

括してデータを送付する処理を実行する。このようなグループは、図４のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図４から明らかなように、１つのグループに含まれる４つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。例えば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１，Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図５Ａに示す

キー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

図５Ａに示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図５Ａ及び図５Ｂの例は、図４に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図４から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図５ＡのＫＲＢに示されるようにＫＲＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図５Ａの下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図５Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図５Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図５Ａの上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図５Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図５Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図５Ａのインデックスは、復号キー

として使用するノードキー、リーフキーの絶対番地を示す。

図４に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０,Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図５Ｂのキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図５Ｂに示すＫＲＢは、例えば特定のグループにおいて共有する新たなマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図４に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図５Ｂに示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

すなわち、デバイス０，１，２，３はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキー:Ｋ（ｔ）masterやメディアキー:Ｋ（ｔ）mediaを得ることが可能になる。

図６に、本出願人の先の特許出願である特願２０００－１０５３２８で提案したｔ時点でのメディアキーＫ（ｔ）mediaを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のメディアキーＫ（ｔ）mediaを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media）と図５Ｂに示すＫＲＢとを記録媒体を介して受領したデバイス２の処理を示す。

図４に示すように、ある記録再生システムには、点線で囲まれた、デバイス０，１，２，３の４つの装置が含まれるとする。図６は、デバイス３がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置（デバイス２）が記録媒体上のコンテンツを暗号化若しくは復号するために必要なメディアキーを、記録媒体に格納されているＫＲＢ（Key Renewal Block）と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表してい

る。

デバイス２のメモリには、自分にのみ割り当てられたリーフキーＫ００１０と、そこから木のルートまでの各ノード００１,００,０,Ｒのノードキー（それぞれ、Ｋ００１,Ｋ００,Ｋ０,ＫＲ）が安全に格納されている。デバイス２は、図６の記録媒体に格納されているＫＲＢのうち、インデックス（index）が００１０の暗号文を自分の持つリーフキーＫ００１０で復号してノード００１のノードキーＫ（ｔ）００１を計算し、次にそれを用いてインデックス（index）が００１の暗号文を復号してノード００のノードキーＫ（ｔ）_００を計算し、最後にそれを用いて暗号文を復号してメディアキーＫ（ｔ）_mediaを計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

図７の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理及び記録媒体に対する記録処理の一例について説明する。

記録再生装置７００は自身の上述したＫＲＢに基づく算出処理によってメディアキーを取得する。

次に、記録再生装置７００は例えば光ディスクである記録媒体７０２に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）を読出し、記録されていなければ、暗号処理手段１５０においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器７００は、次にメディアキー７０１とディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図８に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS (Federal Information Processing Standards

Publications) 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

次に、記録ごとの固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１参照）においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク７０２に記録する。

次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図９に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、デバイスＩＤ（再生機器制限をしない場合）若しくはデバイス固有キー（再生機器制限をする場合）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、メディアキーとディスクＩＤ（Disc ID）とデバイスＩＤ（再生機器制限をしない場合）若しくはデバイス固有キー（再生機器制限をする場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。なお、再生機器制限とは、記録媒体に格納されたコンテンツデータを制限された特定の再生機器においてのみ再生可能とすることを意味する。

なお、上記の説明では、メディアキーとディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、若しくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤ若しくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイ

トルキー（Title Key）を用いずに、メディアキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ若しくはデバイス固有キーからタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

さらに、図７を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第1～４バイトが分離されて出力されるブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロックキー（Block Key）が生成される。

ブロックキー（Block Key）の生成方法の例を図１０に示す。図１０では、いずれも３２ビットのブロックシード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、例えば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにメディアキーとディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスＩＤ、若しくはデバイス固有キーを用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図７の下段に示すように、ブロックシード（Bloc

k Seed）を含むブロックデータの先頭の第1～mバイト（例えばm＝8バイト）は分離（セレクタ１６０８）されて暗号化対象とせず、m＋1バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブッロク・シードとしての第1～４バイトも含まれる。セレクタにより分離された第m＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロックシード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

記録媒体に格納された暗号化コンテンツデータの復号及び再生処理を説明するブロック図１１に示す。

再生処理においては、図７～図１０を用いて説明した暗号化及び記録処理と同様、メディアキーとディスクＩＤからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体７０２から読み取られるブロック単位の暗号化データの復号処理を実行する。

上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、及び記録媒体からの再生時の復号処理においては、ＫＲＢに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、又は復号処理用の鍵を生成する。

なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーをＫＲＢから取得して、これらに基づいてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成としてもよい。さらに、ＫＲＢから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、及び復号処理に用いるキーとして適用することも可能であ

る。

いずれの構成においても、デバイスは、データの記録、再生時において、図６の記録媒体に格納されているＫＲＢに基づく複数回の復号処理により、データの暗号化又は復号に必要な暗号化キー又は該暗号化キー生成用データを算出することが要請される。このＫＲＢ処理に要する計算回数は、前述したように、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。

これらの処理を軽減する本発明における記録再生装置のメディアキーの取り扱い構成を説明する図を図１２に示す。本発明の構成では、ある記録媒体に格納されているＫＲＢから、記録再生装置がメディアキーを計算するところまでは、図６の処理と同様であるが、本発明においては、メディアキーを自分だけが知る鍵、情報記録再生装置固有のキー、例えば木構造において自分だけに割り当てられているリーフキーを用いて暗号化し、あらかじめ記録媒体に用意されている領域に、記録再生装置の識別情報、例えばその記録再生装置に割り当てられたリーフ番号とともに記録する構成とした。図１２のデバイス２は、ＫＲＢの処理によって取得したメディアキーＫ（ｔ）mediaを自身の有するリーフキーＫ００１０で暗号化して、記録媒体に格納する。

このように、ＫＲＢの複数段の復号処理により取得したメディアキーを再度使用する際に、新たに複数段の復号処理を実行することなく、簡単な復号処理のみで取得可能となる。すなわち、同一の記録再生装置がこの記録媒体を２度目以降にアクセスする際には、わざわざＫＲＢを用いて大量の計算を行わなくても、メディアキー格納テーブルに格納されている暗号文を自分の固有鍵で復号することによってメディアキーを得ることが可能となる。また、記録デバイスに格納された暗号化メディアキーは、デバイス２に固有のリーフキーによってのみ復号可能であるので、他のデバイスに記録媒体を装着しても、暗号化メディアキーを復号して取得することはできない。

本発明における記録再生装置が、記録媒体にアクセスする際、すなわち、例えば記録媒体が記録再生装置に装着された際にメディアキーを得るフローを図１３

に示す。図１３の処理フローについて説明する。

ステップＳ１３０１において、記録再生装置は記録媒体に記録されているメディアキー格納テーブルを読み出す。Ｓ１３０２で、メディアキー格納テーブルのインデックス部を見て、自分自身に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければＳ１３０３に進み、あればＳ１３０９に進む。

Ｓ１３０３では、記録再生装置は、記録媒体から、ＫＲＢ（Key Renewal Block）を読み出す。ステップＳ１３０４において、記録再生装置は、ステップＳ１３０３で読み出したＫＲＢと、自身がメモリに格納しているリーフキー（図４のデバイス２におけるＫ００１０）及びノードキー（図４のデバイス２におけるＫ００１,Ｋ００...）を用いて、識別番号：世代（Generation）（図７におけるｔ）のＫＲＢにおけるノード００の鍵Ｋ（ｔ）００を計算する。

ステップＳ１３０５で、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media)、すなわち、Ｋ（ｔ）００を用いてメディアキーＫ（ｔ）mediaを暗号化した値を読み出す。

そしてステップＳ１３０６において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）mediaを計算する。このようにして計算したメディアキーは、その記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

また、ステップＳ１３０７では、自身のみが持つリーフキー（図４のデバイス２におけるＫ００１０）を用いてメディアキーＫ（ｔ）mediaを暗号化する。

ステップＳ１３０８において、Ｓ１３０７で作成した暗号文と、自身の識別情報となる、リーフキーの番号（リーフ番号）００１０を、記録媒体のメディアキー格納テーブルに記録し、処理を終了する。

ステップＳ１３０２において、自身が格納した暗号文がメディアキー格納テーブルに見つかった場合には、Ｓ１３０９に進み、記録再生装置は記録媒体からその暗号文を読み出す。

Ｓ１３１０において、自身のリーフキーを用いてその暗号文を復号することにより、その記録媒体のメディアキーを得る。これをその記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

なお、上記の処理において、ステップS１３０７及びS１３０８の処理は、記録媒体のメディアキー格納テーブルに、新たに一組のインデックス（index）と暗号文を書きこめる場合のみ行う、図１４のようにすることも可能である。

図１４において、S１３０１乃至S１３０６及びS１３０７乃至S１３１０は、それぞれ図１３の同ステップと同様であるので説明は省略する。

ステップS１４０１において、記録再生装置は記録媒体のメディアキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、ステップS１３０７に進み、S１３０８において暗号文をテーブルに記録するが、スペースが残っていなければ、S１３０７及びS１３０８の処理をスキップして終了する。

上述の実施例においては、先の図１２を用いて説明したように、記録媒体に個々の記録再生装置が用いるテーブルを置いたが、本実施例においては、図１５に示すように、個々の記録再生装置内に記憶手段、例えば図１に示す記録再生装置１００のメモリ１８０に、記録媒体ごとのメディアキーを格納する。

記録再生装置１００のメモリ１８０に暗号化処理を施したメディアキーを格納する格納態様は、メディアキーの世代情報をインデックスとして、暗号化処理を施したメディアキーを対応付けたメディアキー格納テーブル構成としている。複数の異なる世代のメディアキーを格納する場合を考慮した構成としている。

上述の実施例と同様の前提において、本実施例における記録再生装置が、記録媒体にアクセスする際、すなわち、例えば記録媒体が記録再生装置に装着された際にメディアキーを得るフローを図１６に示す。

ステップS１６０１において、記録再生装置は記録媒体からそこに格納されているKRB及びメディアキーの識別番号である世代（Generation）（図１５の例ではt）を読み出す。

S１６０２において、記録再生装置は自身内部に格納しているメディアキー格納テーブルにtという世代（Generation）を持つメディアキーが格納されているかどうかを検査する。格納されていなければS１６０３に進み、格納されていればS１６１０に進む。

S１６０３乃至S１６０６の処理は、それぞれ図１３のS１３０３乃至S１３

０６の各処理と同様であるので説明を省略するが、これらの処理の結果、記録再生機器はメディアキーを得る。このようにして計算したメディアキーは、その記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

Ｓ１６０７において、記録再生機器は自身の記録手段のメディアキー格納テーブルに新たにメディアキーを格納するスペースがあるかどうかを確認する。スペースがあればＳ１６０８に進み、なければＳ１６０８及びＳ１６０９の処理をスキップする。

Ｓ１６０８では、図１３のＳ１３０７と同様に、自身のリーフキーを用いてメディアキーを暗号化する。Ｓ１６０９で、上記暗号文を、識別情報：世代（Generation）とともにメディアキー格納テーブルに格納する。

ステップＳ１６０２において、世代（Generation）に対応した暗号文がメディアキー格納テーブルに見つかった場合には、Ｓ１６１０に進み、記録再生装置はメディアキー格納テーブルからその暗号文を読み出す。Ｓ１６１１において、図１３のＳ１３１０と同様に、自身のリーフキーを用いてその暗号文を復号することにより、その記録媒体のメディアキーを得る。これをその記録媒体へのデータの記録及び再生時の暗号化及び復号に使用する。

なお、上記の実施例においては、メディアキー格納テーブルにメディアキーを格納する際に、自身のリーフキーを用いて暗号化するようにしているが、例えばメディアキー格納テーブルの内容が外部に露呈することがなく、安全な記録が行える場合には、必ずしも暗号化は必要ではない。すなわち、図１７のように、ＫＲＢの復号処理によって得られるメディアキーＫ（ｔ）mediaをそのまま、暗号化せずに、インデックスとしての世代（Generation）に対応させて格納する構成としてもよい。この場合は、メディアキーＫ（ｔ）mediaを再度使用する場合は、復号処理が不要となる。

また、上述の実施例を組み合わせて、メディアキー格納テーブルを記録媒体と記録再生装置の両方に持たせるようにすることも可能である。

なお、上述の例では、ＫＲＢ処理に基づいて取得するキーをメディアキーとして説明したが、この方法は、メディアキーに特化したものではなく、例えば複数のデバイスに共通に格納されたマスターキー、デバイス毎に固有のデバイスキー

に適用することももちろん可能である。

なお、上述の例では、鍵を配信するためのデータをキー更新ブロック（ＫＲＢ）という表現を用いて説明したが、キー更新ブロックは、鍵の更新に限られるものではなく、鍵の配布全般に適応可能であることは、上述の説明から明らかである。

次に、図１に示した記録再生装置が、データを記録媒体に記録、若しくは記録媒体から再生する際に必要なキー、例えばコンテンツキーを、各機器に配布する構成について説明する。ここで、コンテンツキーは、通信媒体若しくは記録媒体を介して配布される暗号化されたコンテンツを復号するための鍵である。図１８は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１８の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１８に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーを自身に格納する。図１８の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図１８に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１８のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図１８のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存

することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１８に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１８の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、コンテンツキーを暗号化して送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１８の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１８のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図１８から明らかなように、１つのグループに含まれる４つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通の暗号化コンテンツキーをデバイス０，１，２，３のみに提供することが可能となる。例えば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKcontentをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kcontent）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kcontent）を解いてコンテンツキー：K

contentを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図１９Ａに示すキー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

図１９Ａに示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１９Ａの例は、図１８に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１８から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図１９ＡのＫＲＢに示されるようにＫＲＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１９Ａの下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得る

ことができる。以下順次、図１９Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１９Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１９Ａの上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図１９Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１９Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図１９Ａのインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図１８に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１９Ｂのキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図１９Ｂに示すＫＲＢは、例えば特定のグループにおいて共有するコンテンツキー、又はマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図１８に点線で示すグループ内のデバイス０，１，２，３にコンテンツキーで暗号化したコンテンツを提供するとともに、暗号化処理したコンテンツキーＫ（ｓ）contentを提供する必要があるとする。ここでｓは、コンテンツを識別するためのコンテンツＩＤを示す。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて共通のコンテンツキー：Ｋ（ｓ）contentを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｓ）content）を図１９Ｂに示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキー等、各種キーについても同様である。

すなわち、デバイス０，１，２，３はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキー：Ｋ（ｓ）contentやメ

ディアキー:K（t）mediaを得ることが可能になる。

上述のキー配信構成としてのツリー構造の各リーフに配置された情報記録再生装置に対して音楽データなどのコンテンツをコンテンツキーで暗号化して提供する場合、そのデータ構成は、図２０に示す形態となる。

図２０に示すように、データは、鍵配信部と、コンテンツデータ部とから構成される。鍵配信部は、上述したキー更新ブロック（ＫＲＢ：Key Renewal Block）を有し、さらに、キー更新ブロック（ＫＲＢ）の処理によって得られる更新ノードキーによって暗号化されたコンテンツキー：Ｋ（ｓ）contentを含む構成となっている。コンテンツデータ部は、コンテンツキー：Ｋ（ｓ）contentによって暗号化されたコンテンツ：Ｅｎｃ（Ｋ（ｓ）content，Ｃｏｎｔｅｎｔ）が格納されている。

前述したようにキー更新ブロック（ＫＲＢ）の処理によって更新ノードキーを取得可能な情報記録再生装置は様々に設定することが可能であり、図２０のような暗号化コンテンツの提供構成をとることにより、特定の情報処理装置のみが復号可能なコンテンツを提供することが可能となる。

図２１に、本出願人の先の特許出願である特願２０００－１０５３２９で提案したコンテンツＩＤ＝ｓのコンテンツキーＫ（ｓ）contentにより暗号化されたコンテンツを利用する処理例として、ＫＲＢをＫ００１０を用いて処理し、コンテンツキーＫ（ｓ）contentを取得して、暗号化したデータＥｎｃ（Ｋ（ｓ）content，content）からコンテンツを取得するデバイス２の処理を示す。

図１８に示すように、ある記録再生システムには、点線で囲まれた、デバイス０，１，２，３の４つの装置が含まれるとする。図２１は、デバイス３がリボークされた状態で、コンテンツキーＫ（ｓ）contentを使用する場合に、記録再生装置（デバイス２）において受領するデータの処理を示している。すなわち、コンテンツキーＫ（ｓ）contentを、記録媒体に格納されているＫＲＢ（Key Renewal Block）に基づいて求める際の処理を表している。

デバイス２のメモリには、自分にのみ割り当てられたリーフキーＫ００１０と、そこから木のルートまでの各ノード００１，００，０，Ｒのノードキー（それぞれ、Ｋ００１，Ｋ００，Ｋ０，ＫＲ）が安全に格納されている。デバイス２は、図２１の

記録媒体に格納されているＫＲＢのうち、インデックス（index）が００１０の暗号文を自分の持つリーフキーＫ００１０で復号してノード００１のノードキーＫ（ｔ）００１を計算し、次にそれを用いてインデックス（index）が００１の暗号文を復号してノード００のノードキーＫ（ｔ）００を計算し、次にそれを用いてインデックス（index）が００の暗号文を復号してノード０のノードキーＫ（ｔ）０計算し、最後にそれを用いてインデックス（index）が０の暗号文を復号してノードＲのノードキーＫ（ｔ）Ｒを計算し、さらに、ノードキーＫ（ｔ）Ｒを用いて、Ｅｎｃ（Ｋ（ｔ）Ｒ，Ｋ（ｓ）content）を解いてコンテンツＩＤ＝ｓのコンテンツキーＫ（ｓ）contentを取得する。

その取得したコンテンツキーＫ（ｓ）contentを用いてコンテンツデータ部に格納された暗号化コンテンツ：Ｅｎｃ（Ｋ（ｓ）content，Ｃｏｎｔｅｎｔ）を復号してコンテンツを得る。

このような処理ステップをすべて実行することにより、暗号化コンテンツの復号処理が可能となる。上述のようにキー更新ブロック（ＫＲＢ）の処理によって更新ノードキーを取得する処理は、繰り返し同様の復号処理を実行することが必要であり、この計算回数は、リーフからコンテンツキーを暗号化したノードキーまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。

情報記録再生装置は、コンテンツの再生時において、例えば記録媒体に格納されているＫＲＢに基づく複数回の復号処理により、コンテンツキーを算出することが要請される。例えばコンテンツキーが、コンテンツ毎に異なる鍵として設定されている場合には、それぞれのコンテンツの再生毎に上述のＫＲＢ処理を実行することが必要になる。

これらの処理を軽減する本発明における記録再生装置のコンテンツキーの取り扱い構成を説明する図を図２２に示す。本発明の構成では、ある記録媒体に格納されているＫＲＢから、記録再生装置がコンテンツキーを計算するところまでは、図２１の処理と同様であるが、本発明においては、コンテンツキーを自分だけが知る鍵、すなわち情報記録再生装置固有のキー、例えば木構造において自分だけに割り当てられているリーフキーを用いて暗号化し、例えばあらかじめ記録媒体

に用意されている領域に、記録再生装置の固有キー識別情報、例えばその記録再生装置に割り当てられたリーフ番号とともに記録する構成とした。例えば図２２に示すようにデバイス２の場合、リーフキーを用いて暗号化したコンテンツキー：Ｅｎｃ（Ｋ００１０，Ｋ（ｓ）content）は、図２２に示すように、コンテンツキー格納テーブルとして、対応コンテンツと組にして記録媒体に格納する。

このようなコンテンツキー格納テーブルの格納構成を採用することにより、ＫＲＢの複数段の復号処理により取得したコンテンツキーを再度使用する際、新たに複数段の復号処理を実行することなく、簡単な復号処理のみでコンテンツキーを取得することが可能となる。すなわち、同一の記録再生装置がこの記録媒体を２度目以降にアクセスする際には、わざわざＫＲＢを用いて大量の計算を行わなくても、コンテンツキー格納テーブルに格納している暗号文を自分の固有鍵で復号することによってコンテンツキーを得ることが可能となる。また、デバイスに格納された暗号化コンテンツキーは、そのデバイスに固有のリーフキーによってのみ復号可能であるので、他のデバイスに記録媒体を装着しても、暗号化コンテンツキーを復号して取得することはできない。

本発明における記録再生装置が、コンテンツを利用する際、すなわち、例えば記録媒体が記録再生装置に装着され、暗号化コンテンツキーを取得してコンテンツを復号、再生する処理を示すフローを図２３に示す。図２３の処理フローについて説明する。以下は、記録媒体からのコンテンツの再生に関して説明を行うが、通信媒体からコンテンツを取得する場合であっても同様である。

ステップＳ７０１において、記録再生装置は記録媒体に記録されているコンテンツと一緒に記録されているコンテンツキー格納テーブルを読み出す。

ステップＳ７０２で、コンテンツキー格納テーブルのインデックス部を見て、自分自信に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければＳ７０３に進み、あればＳ７１０に進む。

Ｓ７０３では、記録再生装置は、記録媒体からＫＲＢ（Key Renewal Block）を読み出す。ステップＳ７０４において、記録再生装置は、ステップＳ７０３で読み出したＫＲＢと、自身がメモリに格納しているリーフキー（図１８のデバイス

２においては、Ｋ００１０）及びノードキー（図１８のデバイス２においては、Ｋ００１,Ｋ００...）を用いて、現在自身が再生しようとしているコンテンツの識別番号：コンテンツＩＤ（図２２におけるｔｓ）のＫＲＢにおけるノードRの鍵、すなわちルートキーＫ（ｔ）Ｒを計算する。なお、この例では、ルートキーＫ（ｔ）Ｒにより、コンテンツキーが暗号化されて提供されている例を示しているが、ルートキーより下位のノードキーを用いて、更新ノードキーＫ（ｔ）ｘｘを設定し、その更新ノードキーＫ（ｔ）ｘｘによりコンテンツキーを暗号化して、特定のグループにのみ復号可能なコンテンツキーを配布する構成とした場合は、その更新ノードキーを計算によって算出する。

ステップＳ７０５で、記録媒体からＥｎｃ（Ｋ（ｔ）Ｒ，Ｋ（ｓ）content)、すなわち、Ｋ（ｔ）Ｒを用いてコンテンツキーＫ（ｓ）contentを暗号化した値を読み出す。

そしてステップＳ７０６において、この暗号文をＫ（ｔ）Ｒを用いて復号してＫ（ｓ）contentを計算する。ステップＳ７０７では、記録再生装置は記録媒体上のそのコンテンツのコンテンツキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、Ｓ７０８に進み、スペースが残っていなければ、Ｓ７０８及びＳ７０９の処理をスキップしてＳ７１２に進む。

ステップＳ７０８では、自身のみが持つリーフキー（例えば、図１８のデバイス２においては、Ｋ００１０）を用いてコンテンツキーＫ（ｓ）contentを暗号化する。

ステップＳ７０９において、Ｓ７０８で作成した暗号文と、自身の識別情報となるリーフキーの番号（リーフ番号）００１０（図１８のデバイス２の場合）を、記録媒体のコンテンツキー格納テーブルに記録し、ステップＳ７１２に進む。

一方、ステップＳ７０２において、自身が格納した暗号文がコンテンツキー格納テーブルに見つかった場合には、Ｓ７１０に進み、記録再生装置は記録媒体からその暗号文を読み出す。

Ｓ７１１において、自身のリーフキーを用いてその暗号文を復号することにより、そのコンテンツのコンテンツキーを得て、ステップＳ７１２に進む。ステッ

プＳ７１２では、記録媒体からコンテンツデータ部を読出し、Ｓ７０６又はＳ７１１で得たコンテンツキーを用いて復号することにより平文データを得て、利用する。

このようにすることにより、記録再生機器が、コンテンツを利用するたびにＫＲＢを用いてコンテンツキーを計算する処理を大幅に減少させることが可能となる。

コンテンツを記録媒体に記録する際は、通信媒体又は記録媒体を介して伝送あるいは供給された図２０に示すコンテンツ、すなわちコンテンツデータ部と、鍵配信部を単に記録媒体に記録する。この際に、コンテンツ再生処理と同様、図２３のＳ７０１～Ｓ７０９の処理を行なう。この処理フローを図２４に示す。

図２４のコンテンツ記録時の処理においては、図２３のコンテンツ再生時の処理とほぼ同様の処理が実行される。ステップＳ８０１において、記録再生装置は記録媒体に記録されているコンテンツキー格納テーブルを読み出す。

ステップＳ８０２で、コンテンツキー格納テーブルのインデックス部を見て、自分自身に割り当てられたリーフ番号があるかどうか、すなわち、自分が格納したデータがあるかどうかを検査する。もしそのデータがなければＳ８０３に進み、あればＳ８１２に進む。

Ｓ８０３では、記録再生装置は、記録媒体から、ＫＲＢ（Key Renewal Block）を読み出す。ステップＳ８０４において、記録再生装置は、ステップＳ８０３で読み出したＫＲＢと、自身がメモリに格納しているリーフキー（図１８のデバイス２におけるＫ００１０）及びノードキー（図１８のデバイス２におけるＫ００１,Ｋ００...）を用いて、コンテンツの識別番号：コンテンツＩＤ（図２２におけるｓ）のＫＲＢにおけるノードＲの鍵、すなわちルートキーＫ（ｔ）Ｒを計算する。

ステップＳ８０５で、記録媒体からＥｎｃ（Ｋ（ｔ）Ｒ，Ｋ（ｓ）content）、すなわち、Ｋ（ｔ）Ｒを用いてコンテンツキーＫ（ｓ）contentを暗号化した値を読み出す。

そしてステップＳ８０６において、この暗号文をＫ（ｔ）Ｒを用いて復号してＫ（ｓ）contentを計算する。ステップＳ８０７では、記録再生装置は記録媒体上

のそのコンテンツのコンテンツキー格納テーブルに、自身が記録を行うスペースが残っているかどうかを確認する。スペースが残っていれば、Ｓ８０８に進み、スペースが残っていなければ、Ｓ８０８及びＳ８０９の処理をスキップしてＳ８１２に進む。

また、ステップＳ８０８では、自身のみが持つリーフキー（例えば図１８のデバイス２においては、Ｋ００１０）を用いてコンテンツキーＫ（ｓ）contentを暗号化する。

ステップＳ８０９において、Ｓ８０８で作成した暗号文と、自身の識別情報となる、リーフキーの番号００１０（図１８のデバイス２の場合）を、記録媒体のコンテンツキー格納テーブルに記録し、ステップＳ８１２に進む。

一方、ステップＳ８０２において、自身が格納した暗号文がコンテンツキー格納テーブルに見つかった場合には、Ｓ８０３～Ｓ８０９をスキップしてＳ８１２に進む。

ステップＳ８１２では、通信媒体又は記録媒体を介して伝送あるいは供給されたコンテンツ、すなわちコンテンツキーＫ（ｓ）contentで暗号化されているコンテンツデータ部と、鍵配信部を、そのまま記録媒体に格納する。なお、この例では、コンテンツの格納を最後にしているが、コンテンツはあらかじめ図２０に示すように暗号化されているものであり、Ｓ８０１の前にコンテンツ記録媒体に格納してもよく、コンテンツ格納処理はいつ実行してもよい。

このようにデータ記録時のコンテンツキーを自身の装置固有のキー、例えばリーフキーによって暗号化して記録媒体に格納することにより、その後、記録再生機器がコンテンツを利用する際にＫＲＢを用いてコンテンツキーを計算する処理を大幅に減少させることが可能となる。

上述の実施例においては、先の図２２を用いて説明したように、個々の記録再生装置が用いるコンテンツキー格納テーブルを記録媒体上にコンテンツとともに置いたが、本実施例においては、図２５に示すように、個々の記録再生装置内に記憶手段、例えば図１に示す記録再生装置１００のメモリ１８０に、コンテンツキーを格納する。

記録再生装置１００のメモリ１８０に暗号化処理を施したコンテンツキーを格

納する格納態様は、コンテンツキーのコンテンツＩＤをインデックスとして、暗号化処理を施したコンテンツキーを対応付けたコンテンツキー格納テーブル構成としている。複数の異なるコンテンツＩＤのコンテンツキーを格納する場合を考慮した構成としている。

上述の実施例と同様の前提において、本実施例における記録再生装置が、コンテンツを利用する際、すなわち、例えば暗号化コンテンツが格納された記録媒体が記録再生装置に装着され、暗号化コンテンツを復号して再生するフローを図２６に示す。

ステップＳ１００１において、記録再生装置は記録媒体から、自身が再生しようとしているコンテンツの識別番号であるコンテンツＩＤ.(Content ID)（図２５の例ではｓ）を読み出す。

Ｓ１００２において、記録再生装置は記録装置自身の内部に格納しているコンテンツキー格納テーブルにｓというコンテンツＩＤを持つコンテンツキーが格納されているかどうかを検査する。格納されていなければＳ１００３に進み、格納されていればＳ１０１０に進む。

Ｓ１００３乃至Ｓ１００６の処理は、それぞれ図２３のＳ７０３乃至Ｓ７０６の各処理と同様であるので説明を省略するが、これらの処理の結果、記録再生機器はコンテンツキーを得る。

Ｓ１００７において、記録再生機器は自身の記録手段のコンテンツキー格納テーブルに新たにコンテンツキーを格納するスペースがあるかどうかを確認する。スペースがあればＳ１００８に進み、なければＳ１００８及びＳ１００９の処理をスキップする。

Ｓ１００８では、図２３のＳ７０８と同様に、自身のリーフキーを用いてコンテンツキーを暗号化する。Ｓ１００９で、上記暗号文を、識別情報であるコンテンツＩＤとともにコンテンツキー格納テーブルに格納し、ステップＳ１０１２に進む。

ステップＳ１００２において、コンテンツＩＤに対応した暗号文がコンテンツキー格納テーブルに見つかった場合には、Ｓ１０１０に進み、記録再生装置はコンテンツキー格納テーブルからその暗号文を読み出す。Ｓ１０１１において、図

２３のＳ７１１と同様に、自身のリーフキーを用いてその暗号文を復号することにより、そのコンテンツのコンテンツキーを得て、ステップＳ１０１２に進む。

ステップＳ１０１２では、図２３のＳ７１２と同様に、記録媒体からコンテンツデータ部を読み出し、Ｓ１００６又はＳ１０１１で得たコンテンツキーを用いて暗号化コンテンツの復号処理を実行して、音楽データ等のコンテンツの平文データを得て、再生利用する。

なお、上記の実施例においては、コンテンツキー格納テーブルにコンテンツキーを格納する際に、自身のリーフキーを用いて暗号化するようにしているが、例えばコンテンツキー格納テーブルの内容が外部に露呈することがなく、安全な記録が行える場合には、必ずしも暗号化は必要ではない。また、上記の例では、コンテンツを利用する際にコンテンツキー格納テーブルに自身のリーフキーで暗号化したコンテンツキーを格納するようにしているが、コンテンツを記録媒体に記録する際、すなわち、コンテンツキーを用いてコンテンツを暗号化して記録媒体に格納し、その暗号化に用いたコンテンツキーを上述と同様にコンテンツキー格納テーブルに格納する処理を行う構成としてもよい。

また、上述の実施例を組み合わせて、コンテンツキー格納テーブルを記録媒体と記録再生装置の両方に持たせるようにすることも可能である。

なお、上述の例では、鍵を配信するためのデータをキー更新ブロック（ＫＲＢ）という表現を用いて説明したが、キー更新ブロックは、鍵の更新に限られるものではなく、鍵の配布全般に適応可能であることは、上述の説明から明らかである。

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録

再生を行う場合の図１の記録再生装置の処理について、図２７Ａ、図２７Ｂ及び図２８Ａ、図２８Ｂのフローチャートを参照して説明する。

まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図２７Ａのフローチャートにしたがった記録処理が行われる。図２７Ａの処理について説明する。ここでは、図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE 1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ１８０１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ１８０２に進む。

ステップＳ１８０２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

ステップＳ１８０２において、コンテンツがコピー可能でないと判定された場

合、ステップＳ１８０３～Ｓ１８０４をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

また、ステップＳ１８０２において、コンテンツがコピー可能であると判定された場合、ステップＳ１８０３に進み、以下、ステップＳ１８０３～Ｓ１８０４において、図２Ａのステップ２０２、Ｓ２０３における処理と同様の処理が行われる。すなわち、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図２７Ｂのフローチャートにしたがった記録処理が行われる。図２７Ｂの処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ１８１１において、そのアナログコンテンツを受信し、ステップＳ１８１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップＳ１８１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-gen

eration)、又はコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

ステップＳ１８１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ１８１３乃至Ｓ１８１６をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１９５に記録されない。

また、ステップＳ１８１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ１８１３に進み、以下、ステップＳ１８１３乃至Ｓ１８１６において、図２Ｂのステップ２２２乃至２２５における処理と同様の処理が行われ、これにより、コンテンツがディジタル変換、ＭＰＥＧ符号化、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図２８Ａのフローチャートにしたがった再生処理が行われる。図２８Ａの処理について説明する。最初に、ステップＳ１９０１、Ｓ１９０２において、図３Ａのステップ３０１、３０２における処理

と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、復号処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

入出力Ｉ／Ｆ１２０は、ステップＳ１９０３において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格にしたがって、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＥＭＩ(Recorded EMI)）が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録されたＥＭＩ等のコピー制御情報が、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

ステップＳ１９０３において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ１９０４に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップＳ１９０３において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ１９０５に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等にしたがって、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（若しくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図２８Ｂのフローチャートにしたがった再生処理が行われる。図２８Ｂの処理について説明する。ステップＳ１９１１乃至Ｓ１９１４において、図３Ｂのステップ３２１乃至３２４における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

入出力Ｉ／Ｆ１４０は、ステップＳ１９１５において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにＥＭＩ等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えば、ＤＴＣＰの規格にしたがって、ＥＭＩ等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、ＥＭＩ等のコピー制御情報が、No-more-copiesである場合、若しくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合には、アナログコンテンツは、後でコピー可能なものでないと

判定される。

さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

ステップＳ１９１５において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ１９１６に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップＳ１９１５において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ１９１７に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（若しくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図２９は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク２００５やＲＯＭ２００３に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体２０１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体２０１０は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体２０１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部２００８で受信し、内蔵するハードディスク２００５にインストールすることができる。

コンピュータは、ＣＰＵ(Central Processing Unit)２００２を内蔵している。ＣＰＵ２００２には、バス２００１を介して、入出力インタフェース２０１１が接続されており、ＣＰＵ２００２は、入出力インタフェース２０１０を介して、ユーザによって、キーボードやマウス等で構成される入力部２００７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)２００３に格納されているプログラムを実行する。

あるいは、ＣＰＵ２００２は、ハードディスク２００５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部２００８で受信されてハードディスク２００５にインストールされたプログラム、又はドライブ２００９に装着されたリムーバブル記録媒体２０１０から読み出されてハードディスク２００５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)２００４にロードして実行する。

これにより、ＣＰＵ２００２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ２００２は、その処理結果を、必要に応じて、例えば、入出力インタフェース２０１１を介して、ＬＣＤ(Liquid Crystal Display)やスピーカ等で構成される出力部２００６から出力、あるいは、通信部２００８から送信、さらには、ハードディスク２００５に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

以上、説明したように、本発明の情報記録再生装置によれば、ツリー（木）構造の鍵配布構成により、コンテンツ暗号鍵としての例えばメディアキーの更新データを更新ブロック（ＫＲＢ）とともに送信する構成とし、記録再生装置がある記録媒体のメディアキーを計算して取得した後に、取得したメディアキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して、記録媒体、又は記録再生装置のメモリに格納する構成としたので、記録再生装置が、次にその記録媒体を使用する際に、その暗号化キーを１回復号するだけでメディアキーを計算できる。従って、記録再生装置が記録媒体にアクセスする際に必要となるＫＲＢ復号処理等の計算量を減少させることが可能となる。

また、ツリー（木）構造の鍵配布構成により、コンテンツ暗号鍵としてのコンテンツキーを更新ブロック（ＫＲＢ）とともに送信する構成とし、記録再生装置があるコンテンツのコンテンツキーを計算して取得した後に、取得したコンテンツキーを、その記録再生装置に固有の暗号鍵、例えばリーフキーを用いて暗号化して暗号文を生成し、記録媒体、又は記録再生装置のメモリに格納する構成としたので、記録再生装置が、次にそのコンテンツを使用する際に、その暗号文を１回復号するだけでコンテンツキーを計算できる。従って、記録再生装置がコンテンツの利用毎に必要となっていたＫＲＢ復号処理等の計算量を減少させることが可能となる。

請求の範囲

1．暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、

暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行い、暗号化された復号用キーを記録媒体又は前記情報処理装置内の記憶領域に格納する

ことを特徴とする情報処理装置。

2．前記情報処理装置固有のキーは、前記各情報処理装置固有のリーフキーであることを特徴とする請求の範囲第1項記載の情報処理装置。

3．前記キーブロックは、前記記憶手段に記憶されたノードキーを更新するための更新ノードキーと前記復号用キーを含んでおり、

前記更新ノードキーは、下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーによって暗号化されており、

前記復号用キーは、前記更新ノードキーで暗号化されており、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて前記更新ノードキーを復号して前記更新ノードキーを取得すると共に、前記取得した更新ノードキーを用いて前記復号用キーを算出する

ことを特徴とする請求の範囲第1項記載の情報処理装置。

4．前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて格納することを特徴とする請求の範囲第1項記載の情報処理装置。

５．前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記情報処理装置固有の識別情報と対応付けて格納することを特徴とする請求の範囲第１項記載の情報処理装置。

６．前記暗号処理手段は、前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーで復号される暗号化されたデータの識別情報と対応付けて格納することを特徴とする請求の範囲第１項記載の情報処理装置。

７．前記復号用キーは、前記暗号化されたデータを復号するためのコンテンツキーであることを特徴とする請求の範囲第１項記載の情報処理装置。

８．前記復号用キーは、前記記録媒体に割り当てられたキーであり、暗号化されたデータを復号するために用いられるメディアキーであることを特徴とする請求の範囲第１項記載の情報処理装置。

９．前記復号用キーは、他の情報処理装置と共通に保持されるキーであり、前記暗号化されたデータを復号するために用いられるマスターキーであることを特徴とする請求の範囲第１項記載の情報処理装置。

１０．暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、

暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納する

ことを特徴とする情報処理装置。

１１．暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、

暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するとともに、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納することを特徴とする情報処理装置。

１２．暗号化されたデータを処理する情報処理装置において、

複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを保有する記憶手段と、

復号処理を実行する復号処理手段を有し、

前記復号処理手段は、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、

復号用キーが検出されなかった場合には、前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する

ことを特徴とする情報処理装置。

１３．前記復号処理手段は、復号用キーが検出されなかった場合には、前記記憶手段に保有した前記ノードキー又はリーフキーの少なくともいずれかを用いて算出した前記復号用キーに対して前記情報処理装置固有のキーを用いた暗号化処理を行い、前記記録媒体又は前記情報処理装置内の記憶領域に格納することを特徴

とする請求の範囲第１２項記載の情報処理装置。

１４．前記復号処理手段は、復号用キーが検出された場合には、前記各情報処理装置固有のキーを用いて暗号化された復号用キーを復号することを特徴とする請求の範囲第１２項記載の情報処理装置。

１５．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行い、

暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納する

ことを特徴とする情報処理方法。

１６．前記情報処理装置固有のキーは、前記各情報処理装置固有のリーフキーであることを特徴とする請求の範囲第１５項記載の情報処理方法。

１７．前記キーブロックは、前記情報処理装置に保有されたノードキーを更新するための更新ノードキーと前記復号用キーを含んでおり、

前記更新ノードキーは、下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーによって暗号化されており、

前記復号用キーは、前記更新ノードキーで暗号化されており、

前記キーブロックの復号処理は、前記情報処理装置に保有された前記ノードキー又はリーフキーの少なくともいずれかを用いて前記更新ノードキーを復号して前記更新ノードキー取得する処理であり、

前記復号用キーの算出処理は、前記取得した更新ノードキーを用いて前記復号用キーを算出する処理である

ことを特徴とする請求の範囲第１５項記載の情報処理方法。

１８．前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて格納することを特徴とする請求の範囲第１５項記載の情報処理方法。

１９．前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記情報処理装置固有の識別情報と対応付けて格納することを特徴とする請求の範囲第１５項記載の情報処理方法。

２０．前記情報処理装置固有のキーを用いて暗号化された前記復号用キーを、前記復号用キーで復号される暗号化されたデータの識別情報と対応付けて格納することを特徴とする請求の範囲第１５項記載の情報処理方法。

２１．前記復号用キーは、前記暗号化されたデータを復号するためのコンテンツキーであることを特徴とする請求の範囲第１５項記載の情報処理方法。

２２．前記復号用キーは、前記記録媒体に割り当てられたキーであり、暗号化されたデータを復号するために用いられるメディアキーであることを特徴とする請求の範囲第１５項記載の情報処理方法。

２３．前記復号用キーは、他の情報処理装置と共通に保持されるキーであり、前記暗号化されたデータを復号するために用いられるマスターキーであることを特徴とする請求の範囲第１５項記載の情報処理方法。

２４．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納する

ことを特徴とする情報処理方法。

２５．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行し、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行し、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納することを特徴とする情報処理方法。

２６．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において処理される情報処理方法において、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込み、

前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索し、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出し、

復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーを算出する

ことを特徴とする情報処理方法。

２７．復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて算出した前記復号用キーに対して前記情報処理方法固有のキーを用いた暗号化処理を行い、前記記録媒体又は前記情報処理装置内の記憶領域に格納することを特徴とする請求

の範囲第２６項記載の情報処理方法。

２８．復号用キーが検出された場合には、前記各情報処理装置固有のキーを用いて暗号化された復号用キーを復号することを特徴とする請求の範囲第２６項記載の情報処理方法。

２９．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーに対して、前記情報処理装置固有のキーを用いた暗号化処理を行うステップと、

暗号化された復号用キーを記録媒体又は前記情報処理方法内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

３０．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーを、前記復号用キーの更新情報としての世代番号と対応付けて前記情報処理装置内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

３１．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノ

ードに固有のノードキーと各情報処理方法固有のリーフキーとを保有する情報処理装置において実行されるコンピュータ・プログラムであって、

前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行するステップと、

暗号化されたデータを復号処理する際に用いられる復号用キーの算出処理を実行するステップと、

前記算出した復号用キーを、前記復号用キーを用いて復号される前記データを識別するための識別情報と対応付けて前記情報処理装置内の記憶領域に格納するステップと

を具備することを特徴とするコンピュータ・プログラム。

３２．複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理方法固有のリーフキーとを保有し、暗号化されたデータを処理する情報処理装置において実行されるコンピュータ・プログラムであって、

記録媒体又は情報処理装置内の記憶領域に格納されたテーブルを読み込むステップと、

前記暗号化されたデータの復号処理に用いられる復号用キーが格納されているか否かを検索するステップと、

復号用キーが検出された場合には、前記記録媒体又は前記情報処理装置内の記憶領域に格納された暗号化された復号用キーの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップと、

復号用キーが検出されなかった場合には、前記情報処理装置に保有されている前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー格納データとして構成されるキーブロックの復号処理を実行して、暗号化されたデータを復号処理する際に用いられる復号用キーの算出するステップと

を具備することを特徴とするコンピュータ・プログラム。

３３．記録された情報が情報処理装置によって読み出し可能なように構成された情報記録媒体であって、

前記情報処理装置に固有のキーによって暗号化処理を施した、暗号化されたデータを復号するための復号用キーが、前記情報処理装置の識別情報と関連付けてキー格納テーブルとして記録されていることを特徴とする情報記録媒体。

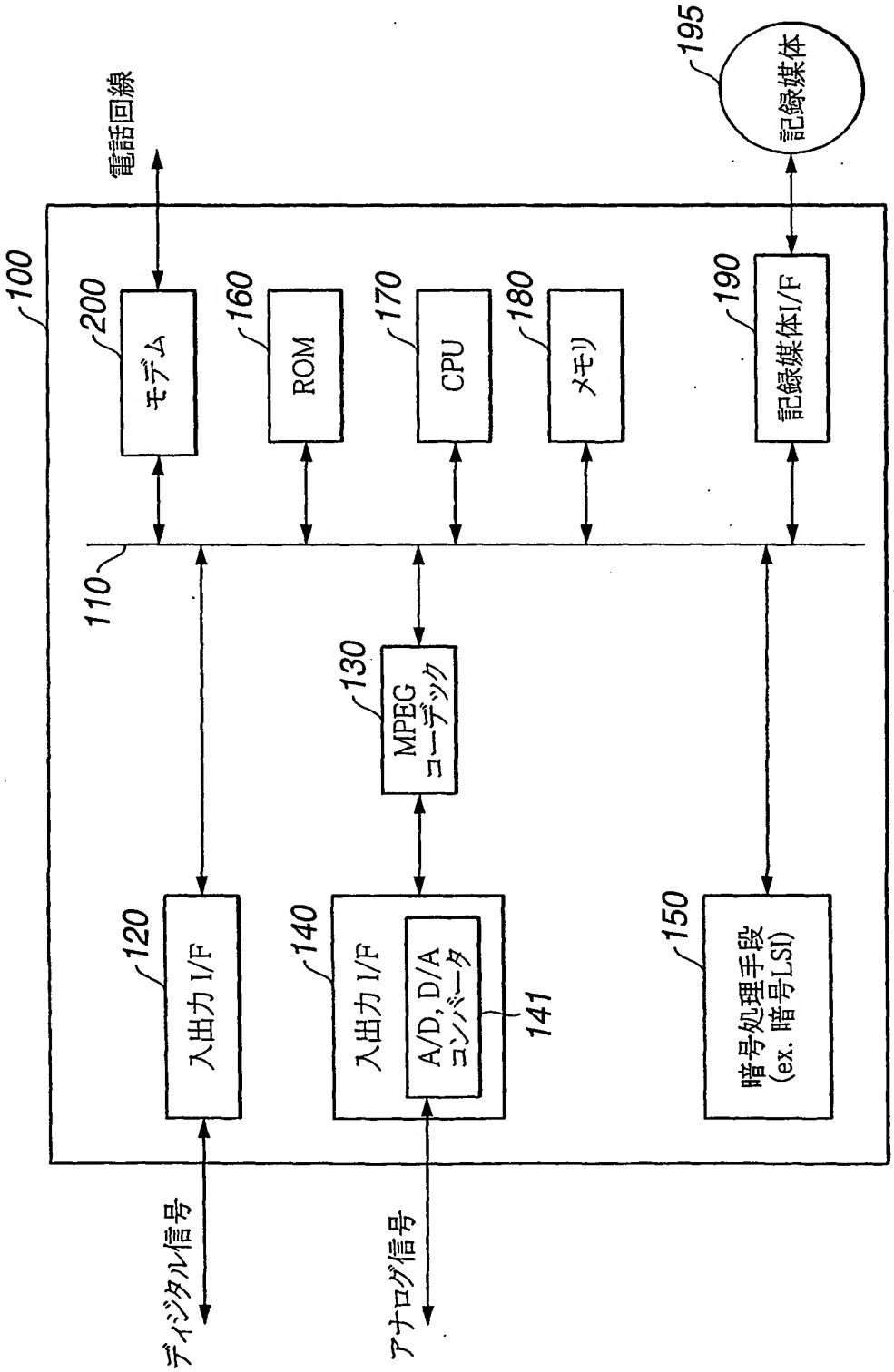

100
電話回線
195
記録媒体
200
モデム
160
ROM
170
CPU
180
メモリ
190
記録媒体I/F
110
130
MPEG
コーデック
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.1

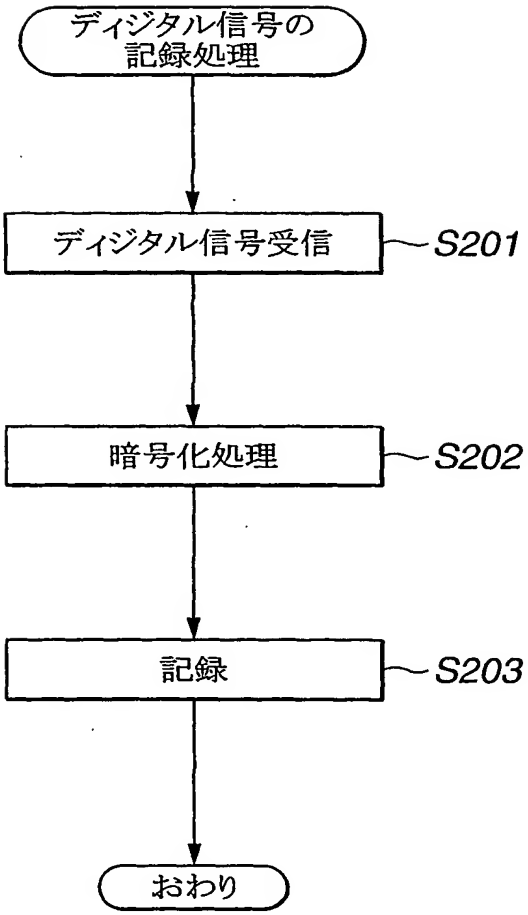

ディジタル信号の
記録処理
ディジタル信号受信
S201
暗号化処理
S202
記録
S203
おわり

FIG.2A

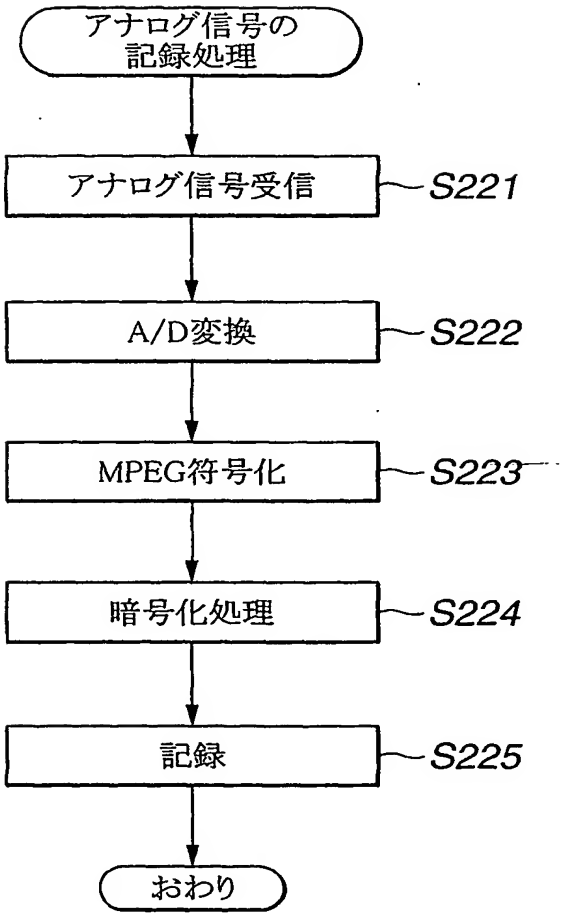

アナログ信号の
記録処理
アナログ信号受信
S221
A/D変換
S222
MPEG符号化
S223
暗号化処理
S224
記録
S225
おわり

FIG.2B

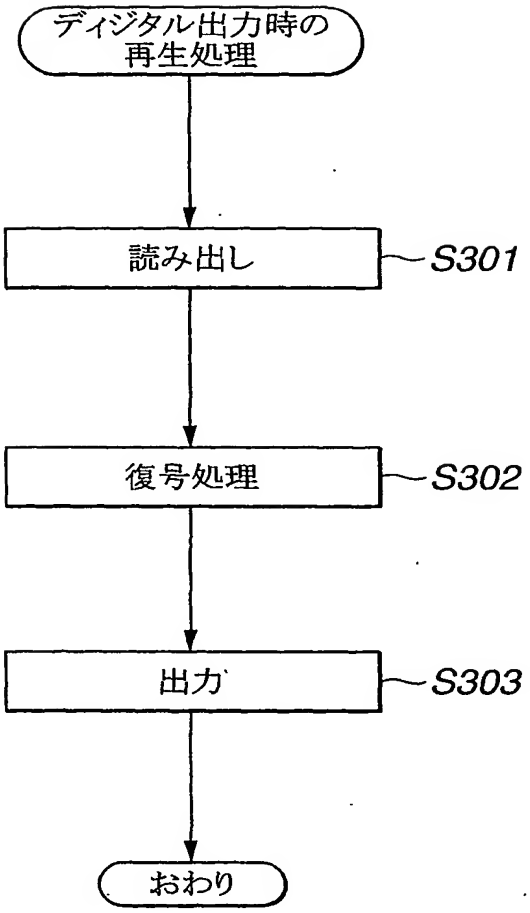

ディジタル出力時の
再生処理
読み出し
S301
復号処理
S302
出力
S303
おわり

FIG.3A

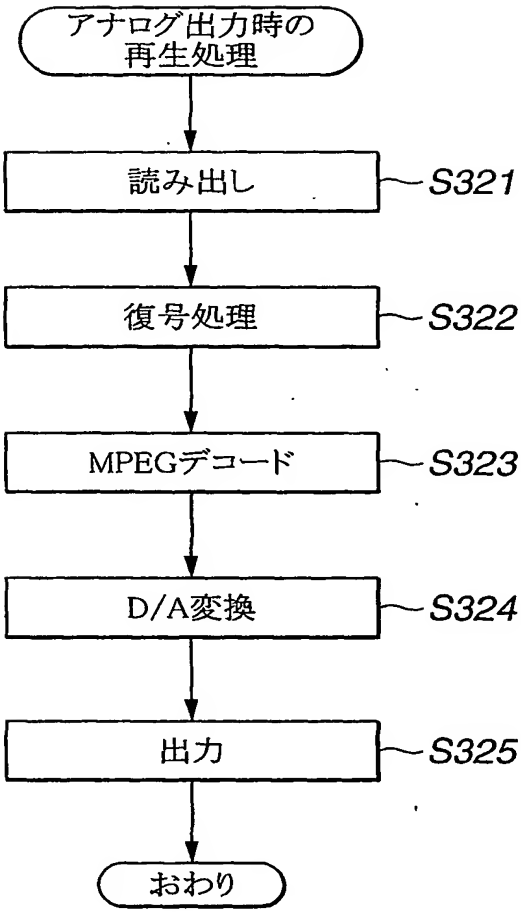

アナログ出力時の
再生処理
読み出し
S321
復号処理
S322
MPEGデコード
S323
D/A変換
S324
出力
S325
おわり

FIG.3B

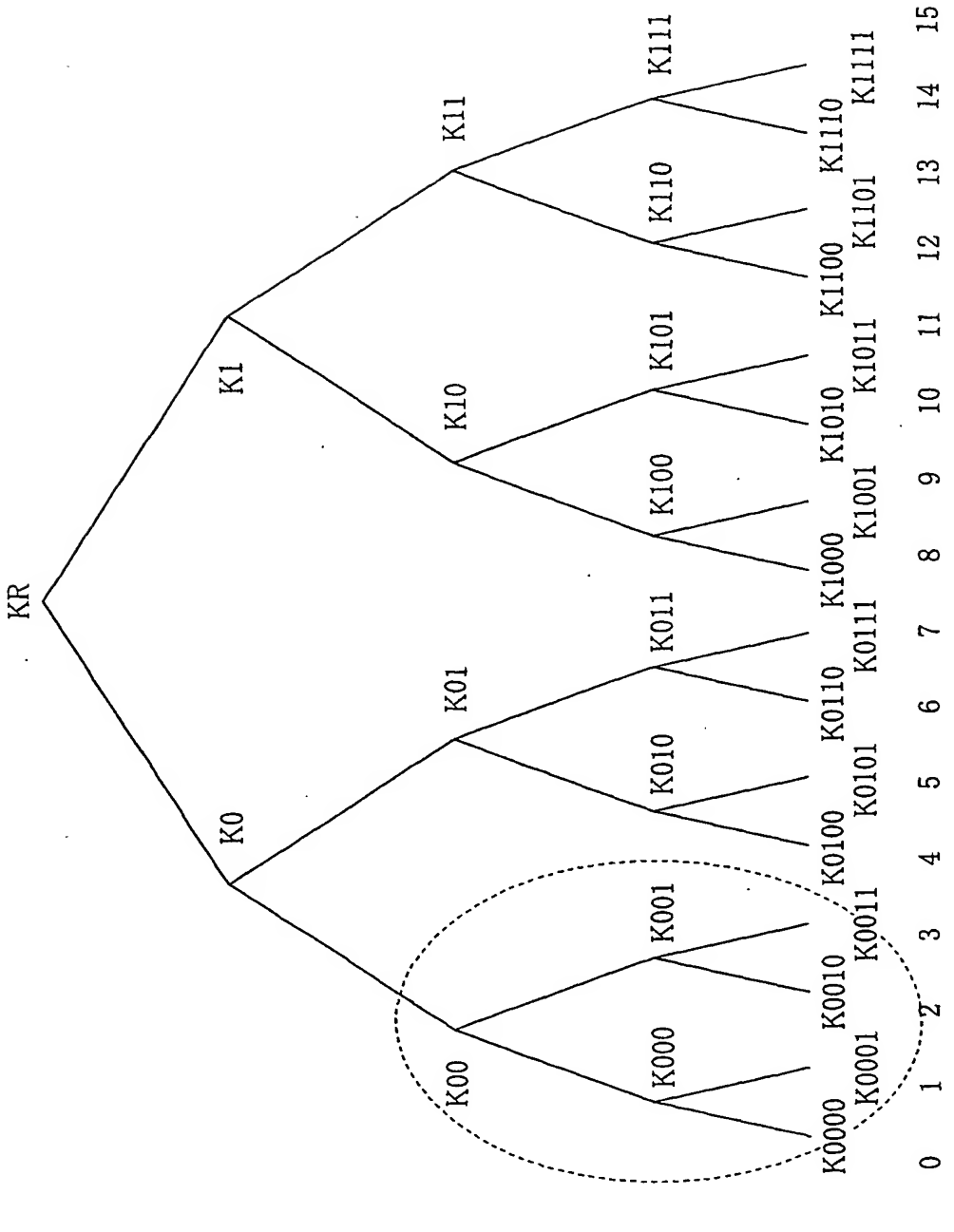

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

FIG.4

キー更新ブロック(KRB : Key Renewal Block) 例1

デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5A

キー更新ブロック(KRB : Key Renewal Block) 例2

デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5B

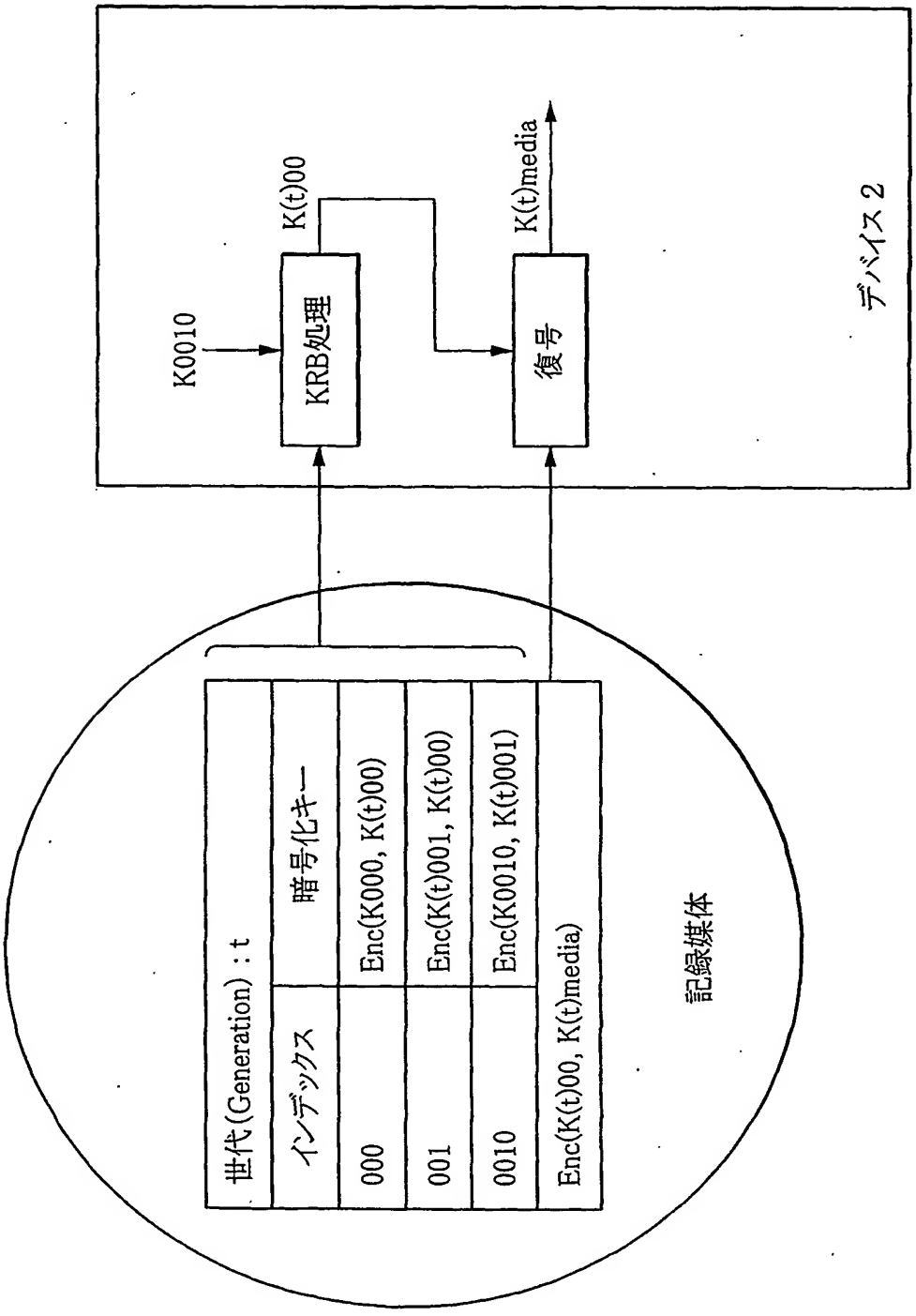

デバイス 2
K0010
KRB処理
K(t)00
復号
K(t)media
記録媒体
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG.6

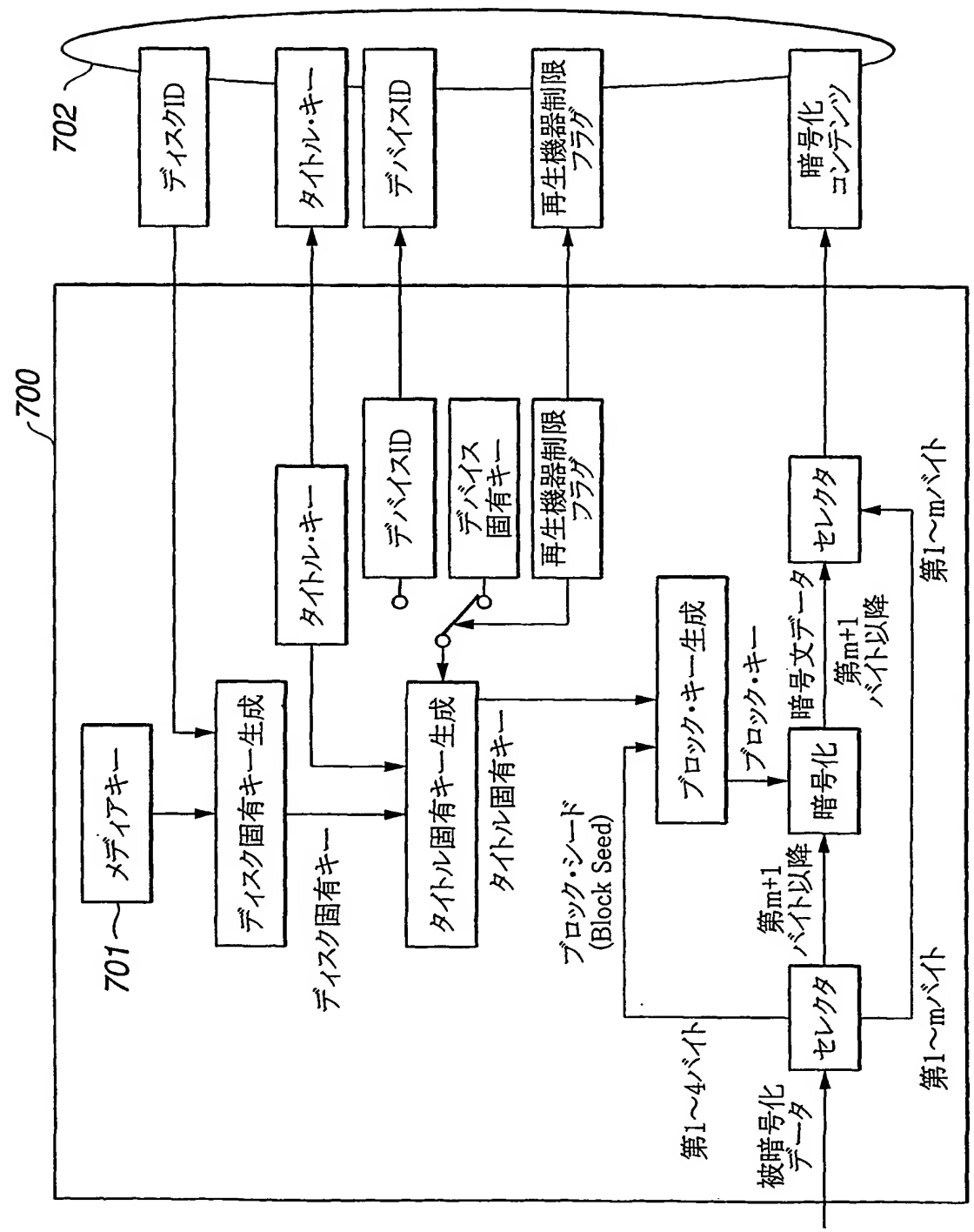

700
701
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル固有キー生成
タイトル固有キー
ブロック・シード
(Block Seed)
ブロック・キー生成
ブロック・キー
暗号化
暗号文データ
セレクタ
第m+1
バイト以降
第1～mバイト
第1～4バイト
セレクタ
被暗号化
データ
第m+1
バイト以降
第1～mバイト
タイトル・キー
デバイスID
デバイス
固有キー
再生機器制限
フラグ
タイトル・キー
デバイスID
再生機器制限
フラグ
暗号化
コンテンツ
ディスクID
702

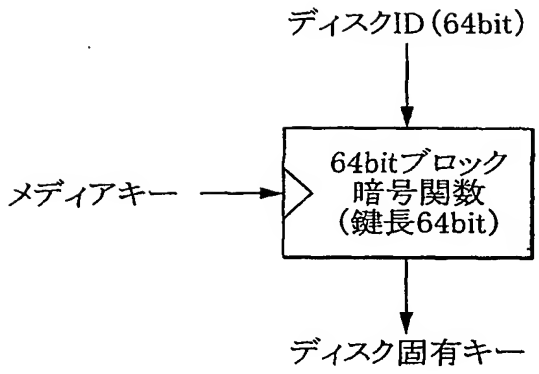
FIG.7

ディスク固有キー生成例

入力
メディアキー(64bit)
ディスクID(64bit)

出力
ディスク固有キー(64bit)

例1



例2

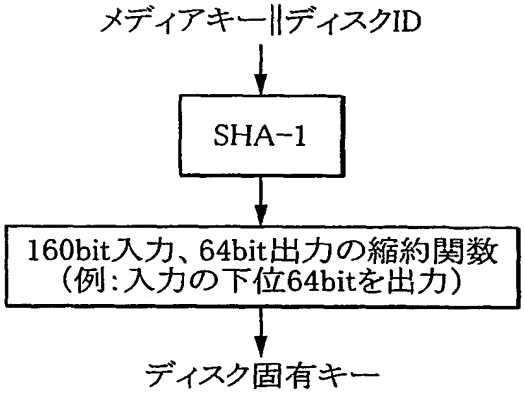


FIG.8

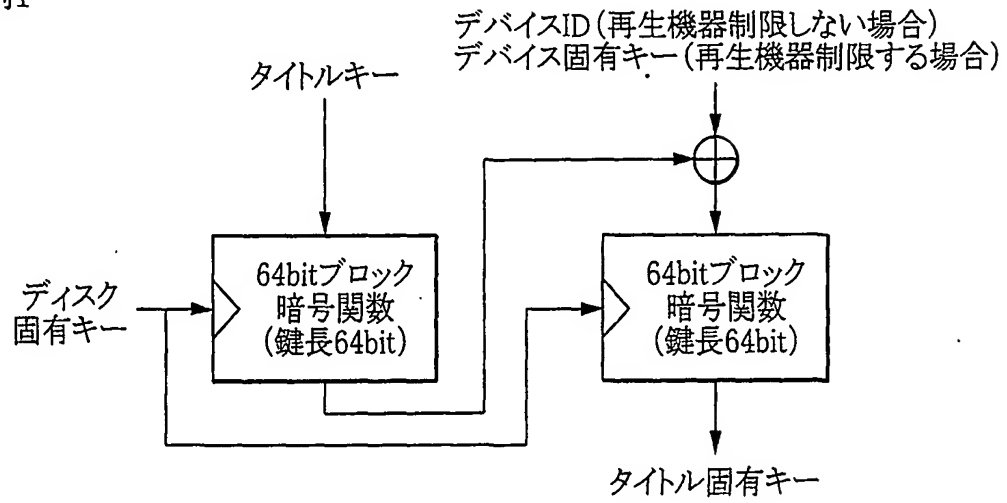
タイトル固有キー生成例

入力
ディスク固有キー(64bit)
タイトルキー(64bit)

ディスクID(64bit)または
デバイス固有キー(64bit)

出力
タイトル固有キー(64bit)

例1



例2

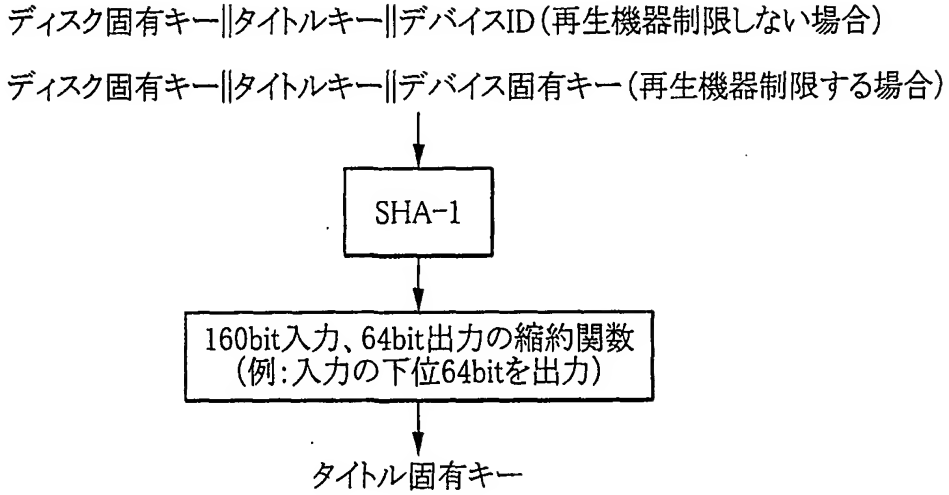


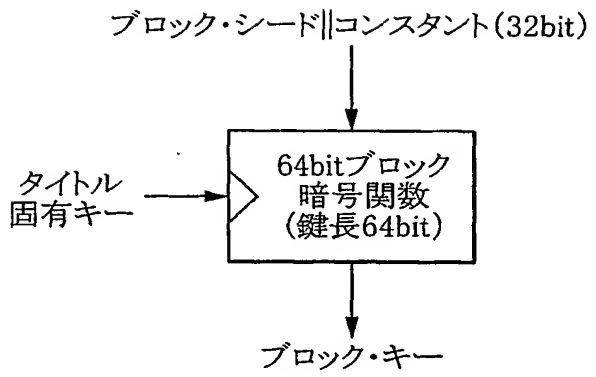
FIG.9

ブロック・キー生成例

入力
ブロック・シード(32bit)
タイトル固有キー(64bit)

出力
ブロック・キー(64bit)

例1



例2

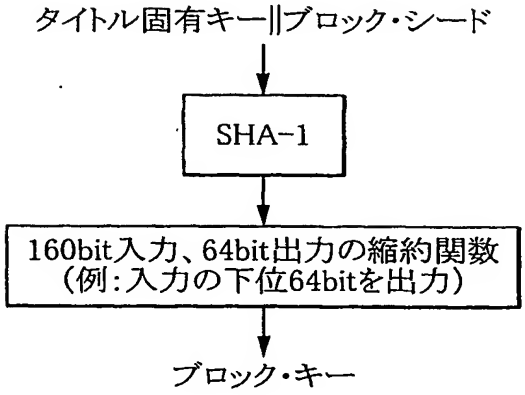


FIG.10

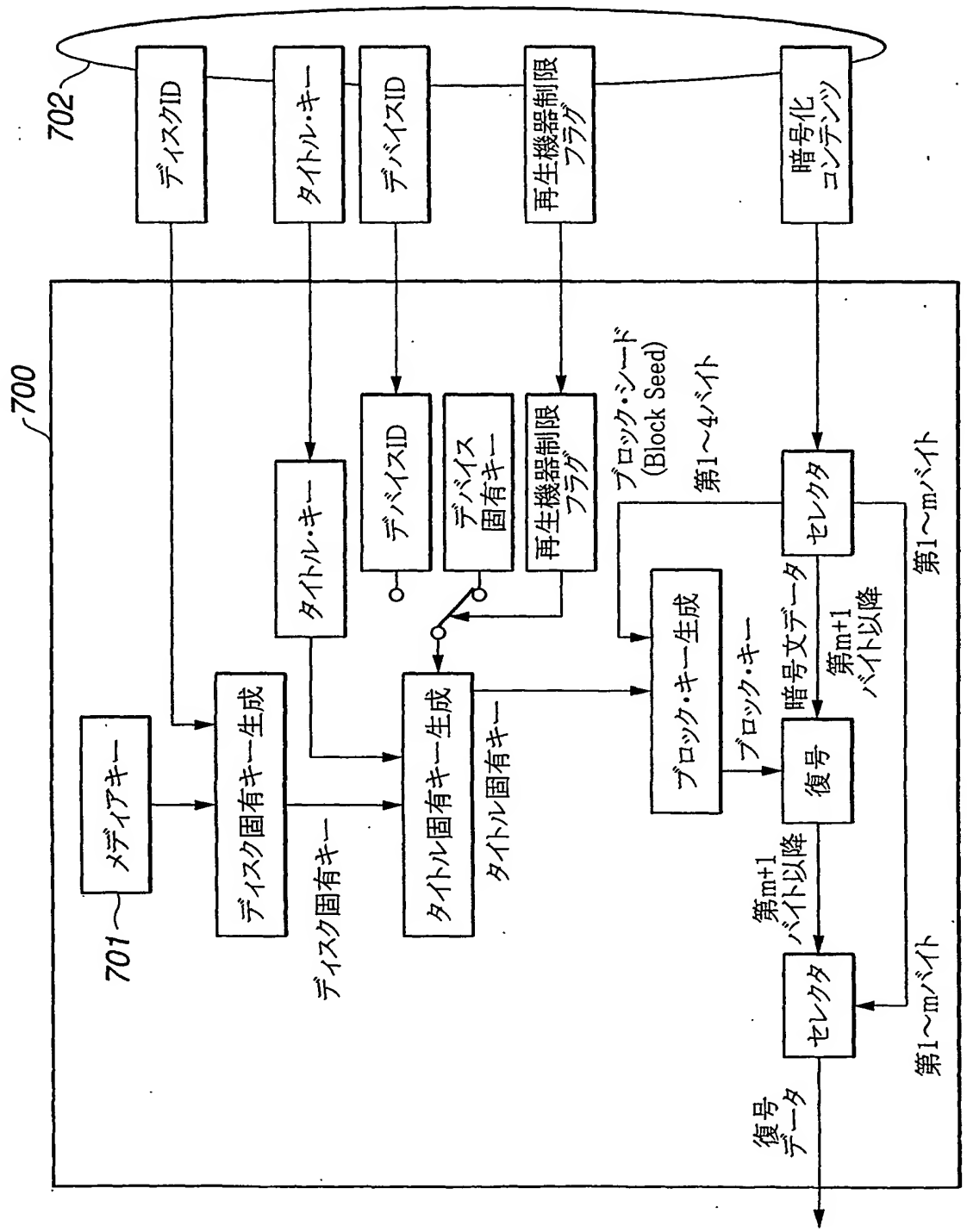

702
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
700
メディアキー
701
ディスク固有キー生成
ディスク固有キー
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー生成
ブロック・キー
セレクタ
暗号文データ
第m+1バイト以降
第1～mバイト
復号
第m+1バイト以降
セレクタ
第1～mバイト
復号データ

FIG.11

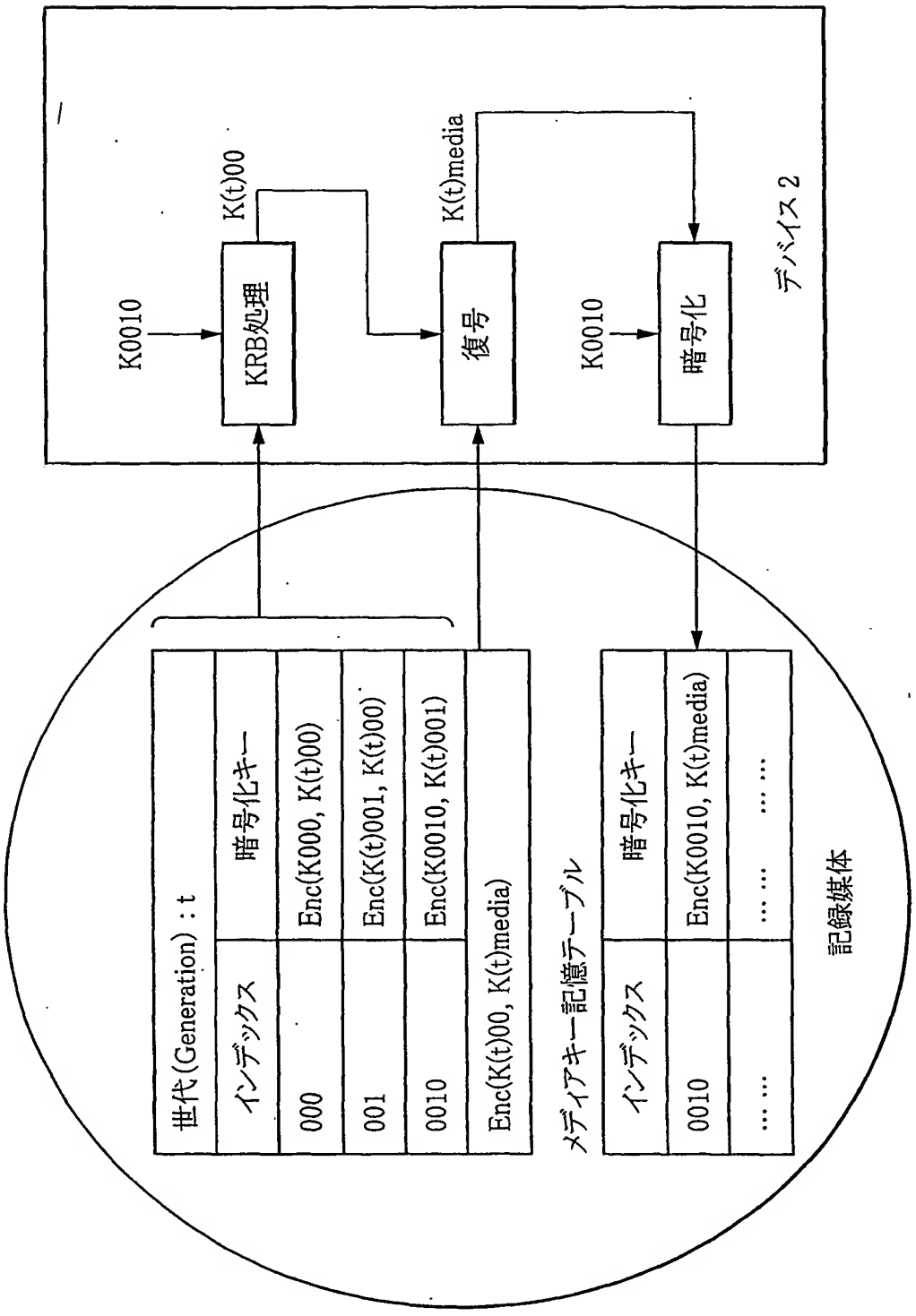

K0010
KRB処理
K(t)00
復号
K(t)media
K0010
暗号化
デバイス 2
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
メディアキー記憶テーブル
インデックス
暗号化キー
0010
Enc(K0010, K(t)media)
記録媒体

FIG.12

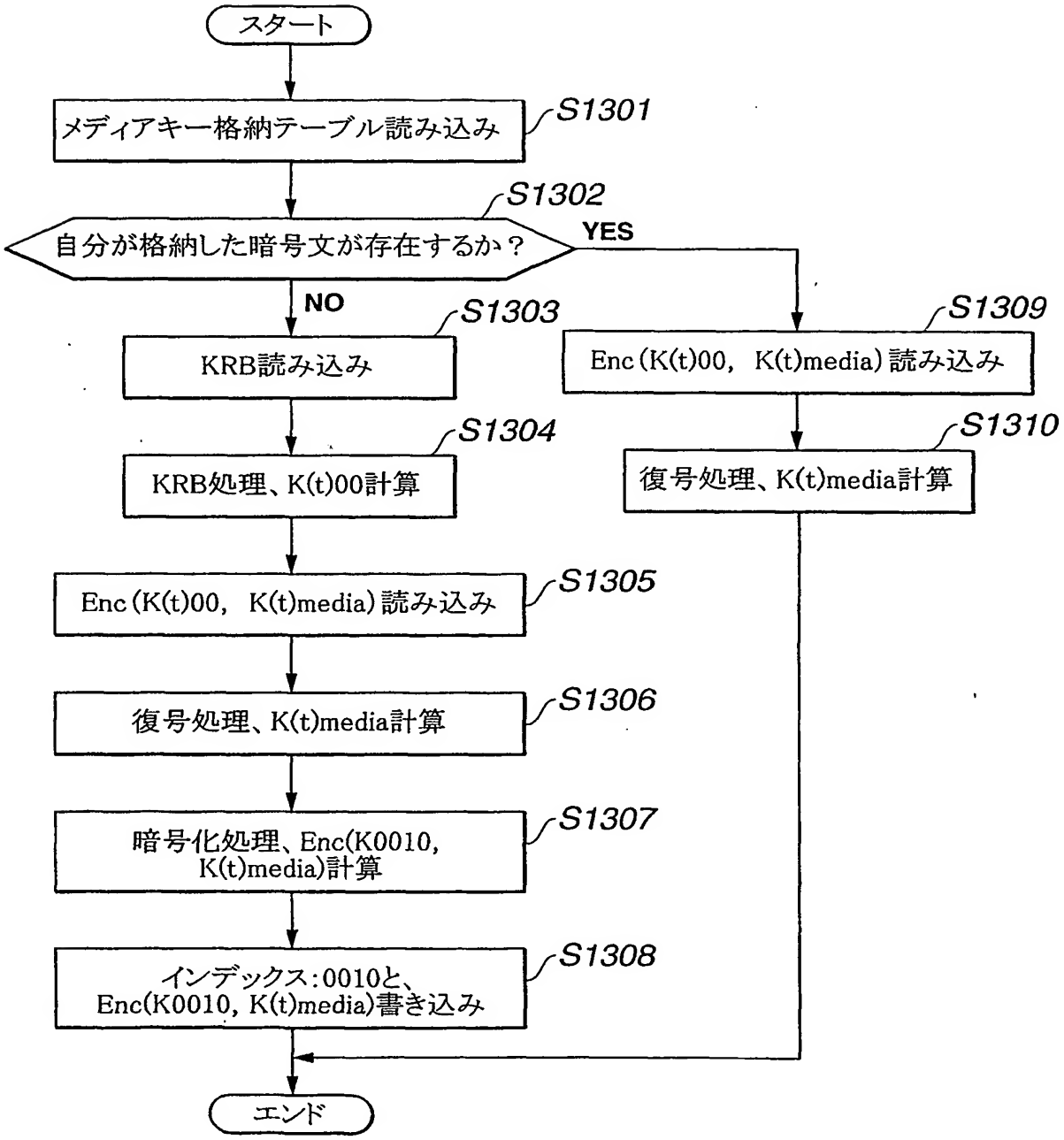

スタート
メディアキー格納テーブル読み込み
S1301
S1302
自分が格納した暗号文が存在するか？
YES
NO
S1303
KRB読み込み
S1304
KRB処理、K(t)00計算
S1309
Enc (K(t)00, K(t)media) 読み込み
S1310
復号処理、K(t)media計算
Enc (K(t)00, K(t)media) 読み込み
S1305
復号処理、K(t)media計算
S1306
暗号化処理、Enc(K0010, K(t)media)計算
S1307
インデックス:0010と、Enc(K0010, K(t)media)書き込み
S1308
エンド

FIG.13

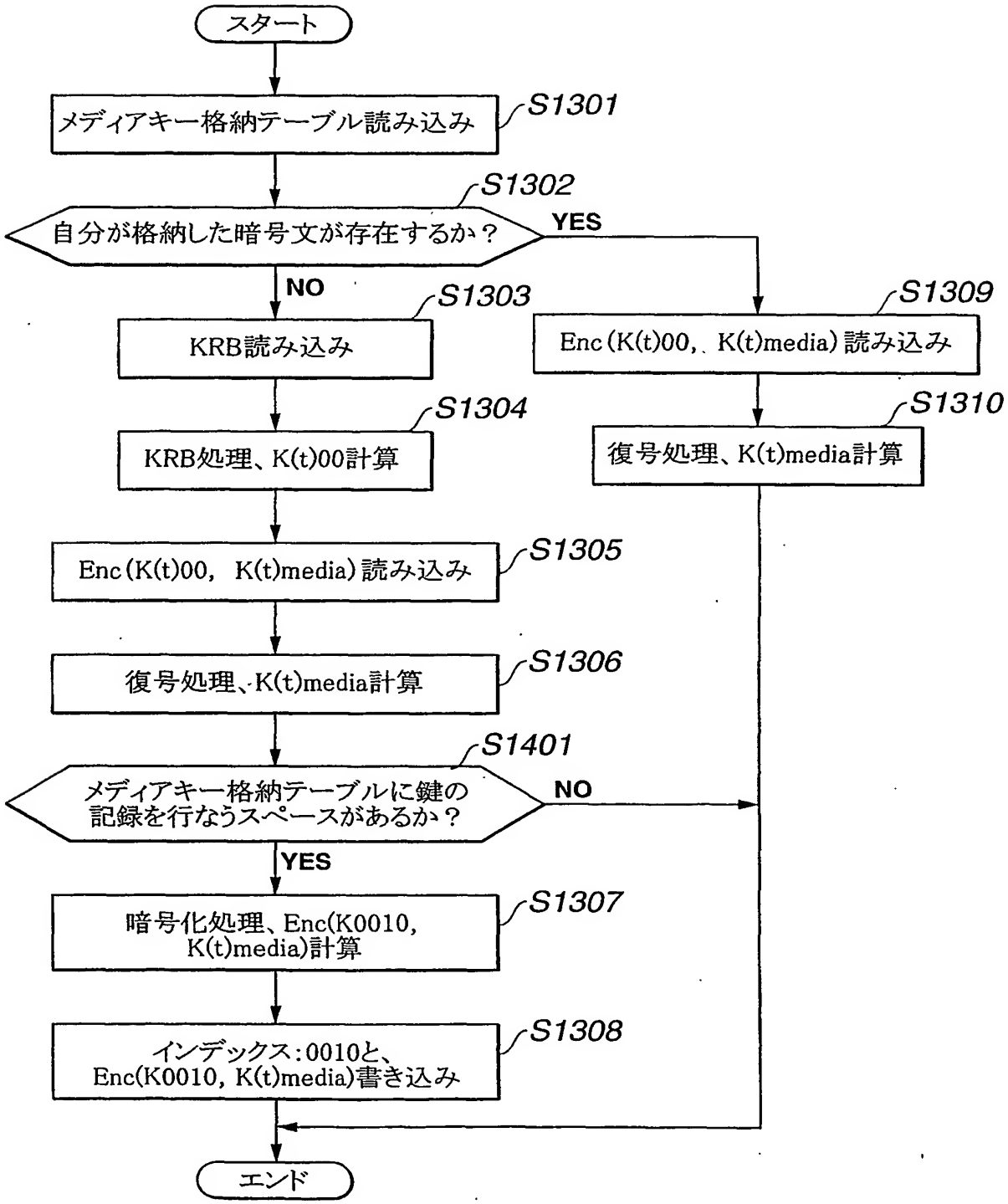

スタート
メディアキー格納テーブル読み込み
S1301
S1302
自分が格納した暗号文が存在するか？
YES
NO
S1303
KRB読み込み
S1304
KRB処理、K(t)00計算
S1309
Enc(K(t)00、K(t)media)読み込み
S1310
復号処理、K(t)media計算
Enc(K(t)00, K(t)media)読み込み
S1305
復号処理、K(t)media計算
S1306
S1401
メディアキー格納テーブルに鍵の記録を行なうスペースがあるか？
NO
YES
暗号化処理、Enc(K0010, K(t)media)計算
S1307
インデックス:0010と、Enc(K0010, K(t)media)書き込み
S1308
エンド

FIG.14

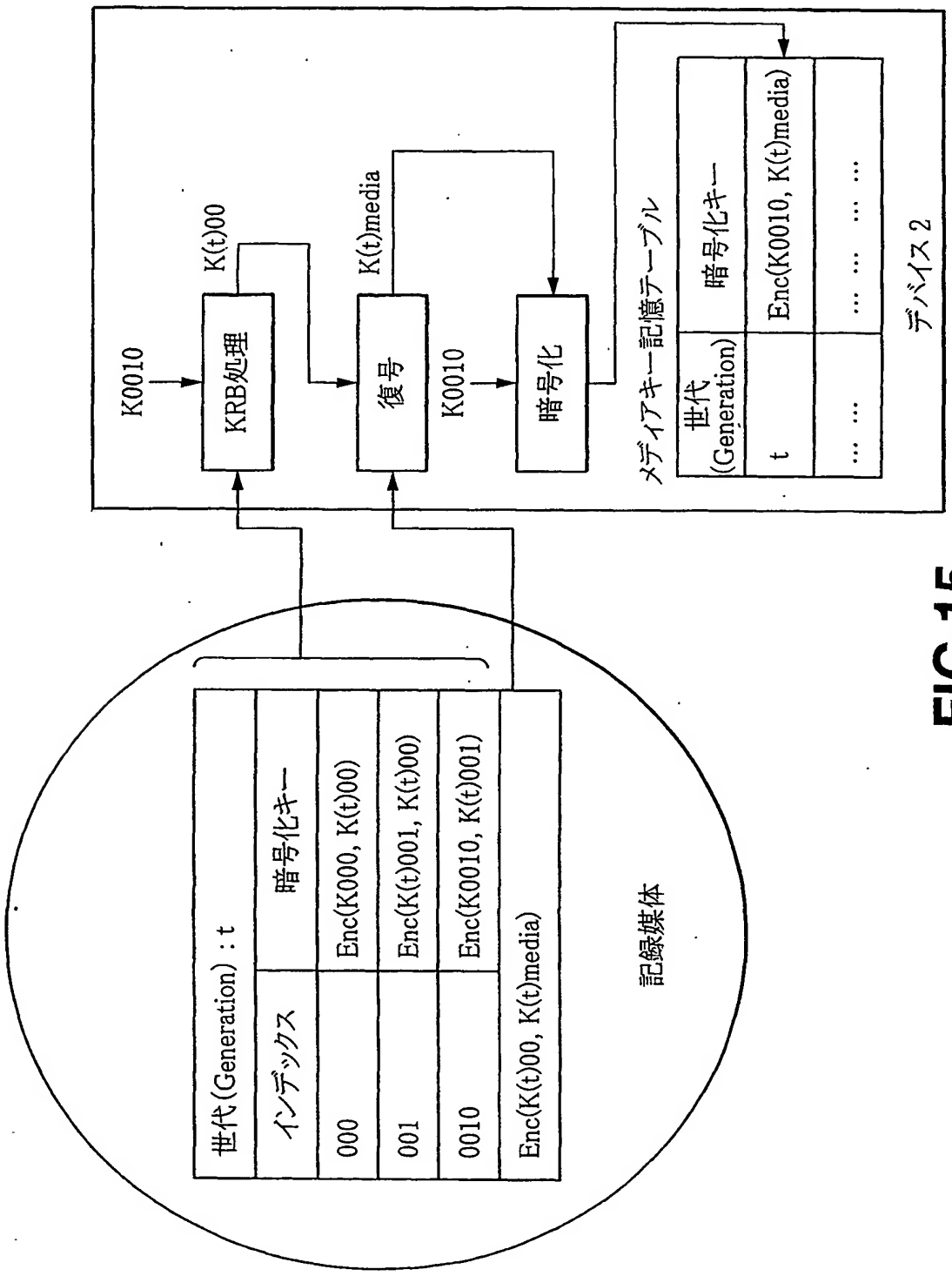

K0010
KRB処理
K(t)00
復号
K(t)media
K0010
暗号化
メディアキー記憶テーブル
世代 (Generation)
暗号化キー
t
Enc(K0010, K(t)media)
デバイス 2
記録媒体
世代 (Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG.15

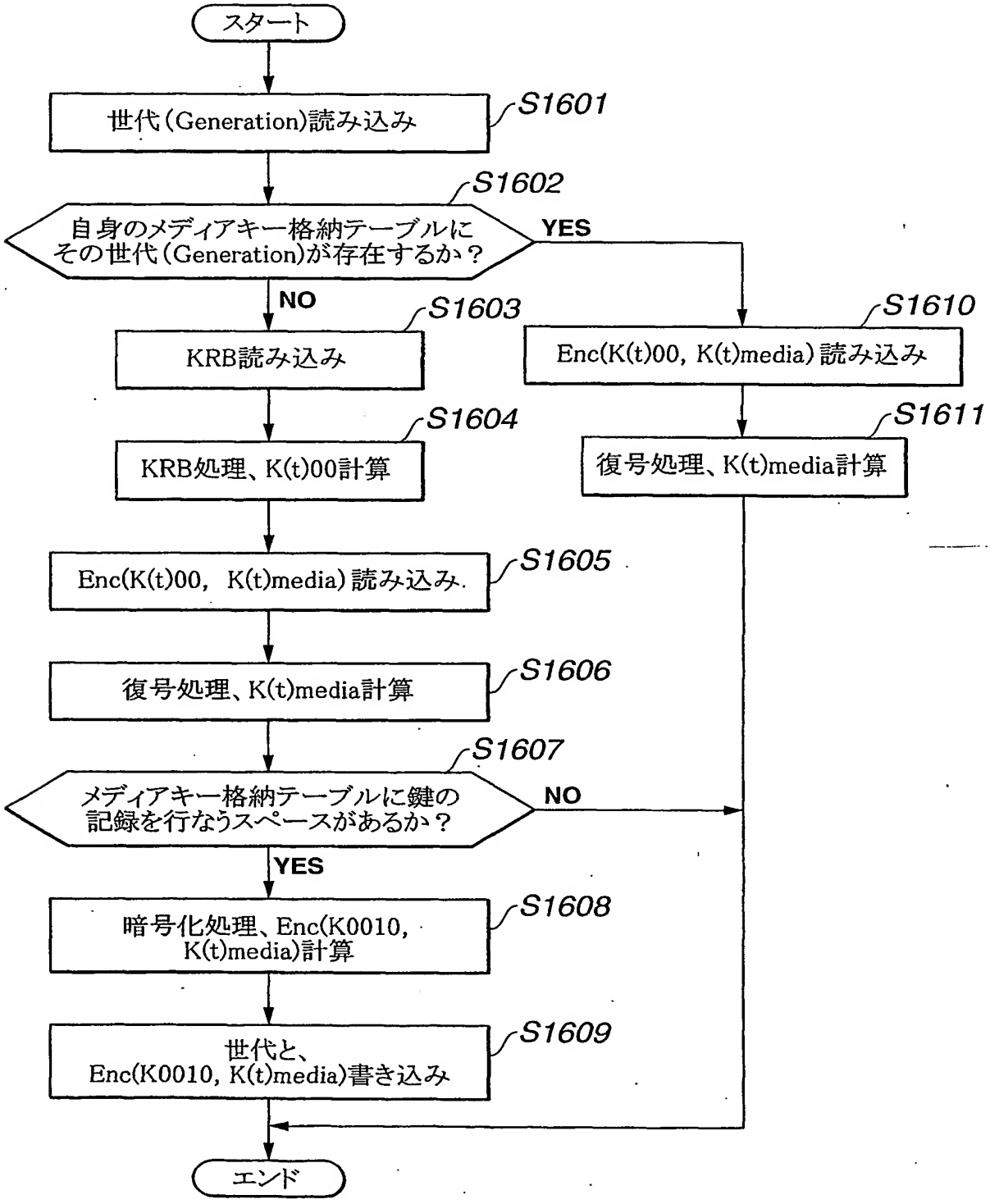

スタート
世代(Generation)読み込み
S1601
S1602
自身のメディアキー格納テーブルに
その世代(Generation)が存在するか？
YES
NO
S1603
KRB読み込み
S1604
KRB処理、K(t)00計算
Enc(K(t)00, K(t)media)読み込み.
S1605
復号処理、K(t)media計算
S1606
S1607
メディアキー格納テーブルに鍵の
記録を行なうスペースがあるか？
NO
YES
暗号化処理、Enc(K0010,
K(t)media)計算
S1608
世代と、
Enc(K0010, K(t)media)書き込み
S1609
S1610
Enc(K(t)00, K(t)media)読み込み
S1611
復号処理、K(t)media計算
エンド

FIG.16

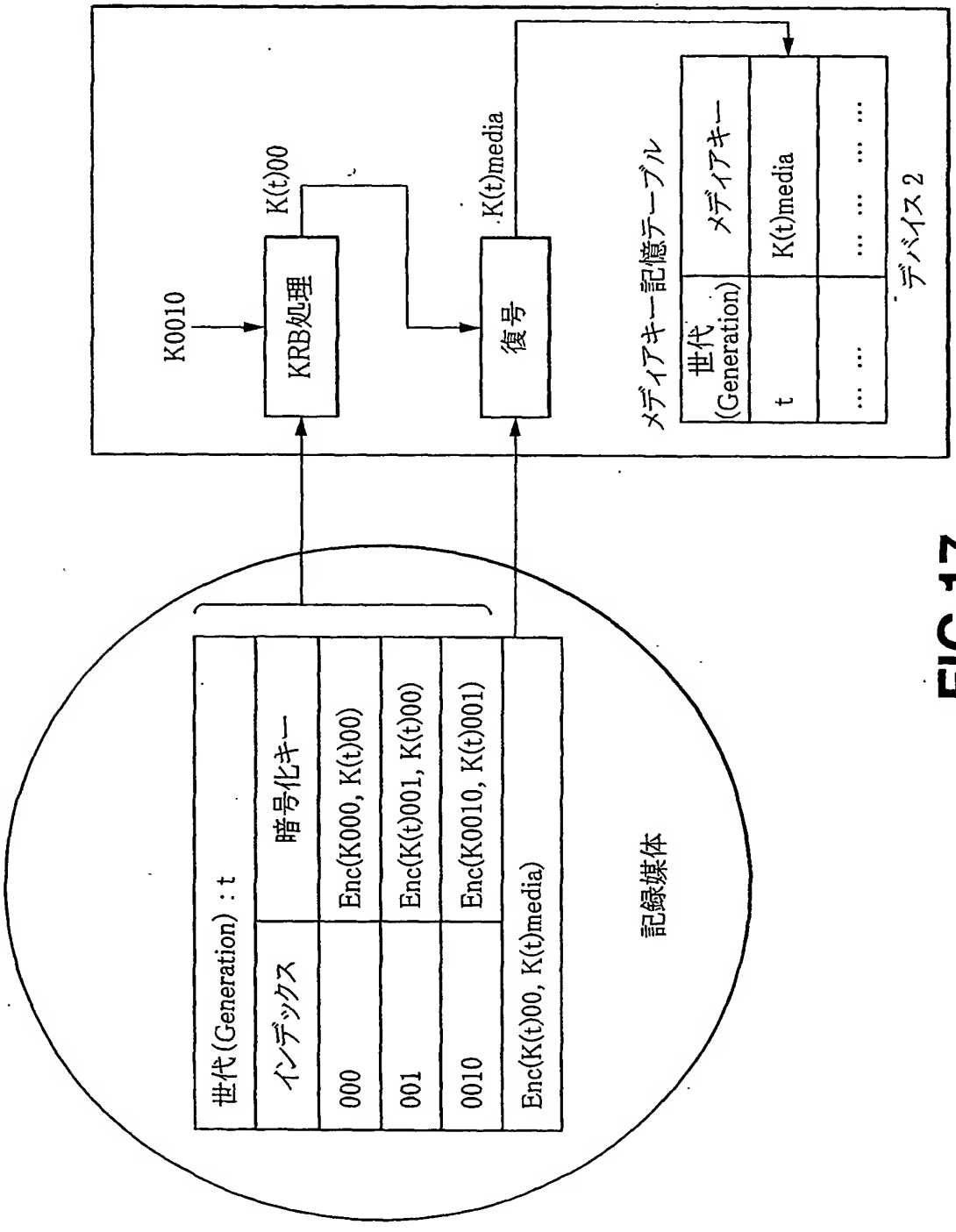

K0010
KRB処理
K(t)00
復号
K(t)media
メディアキー記憶テーブル
世代 (Generation)
メディアキー
t
K(t)media
デバイス 2
記録媒体
世代 (Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG.17

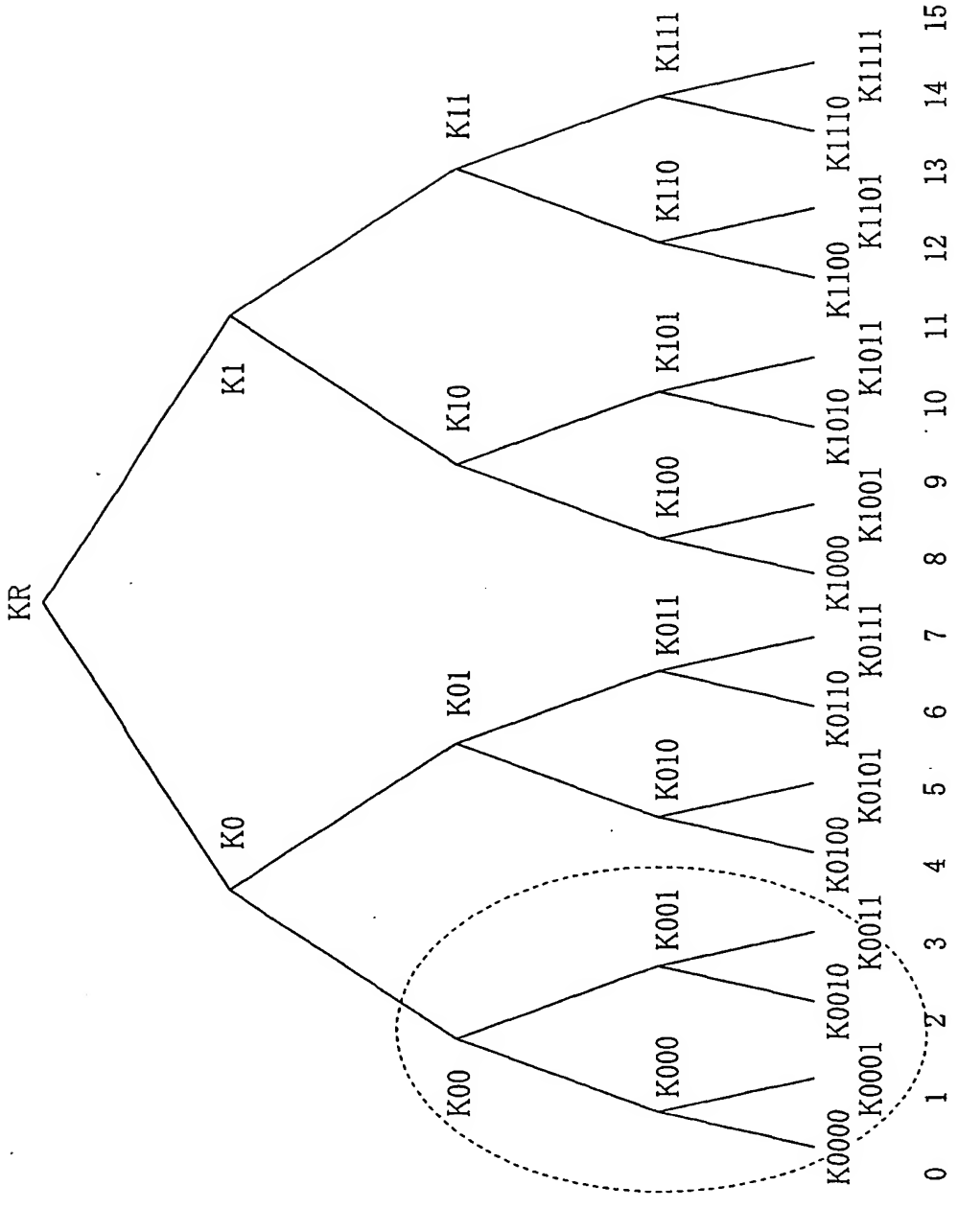

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

FIG.18

キー更新ブロック(KRB : Key Renewal Block) 例1

デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.19A

キー更新ブロック(KRB : Key Renewal Block) 例2

デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代(Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.19B

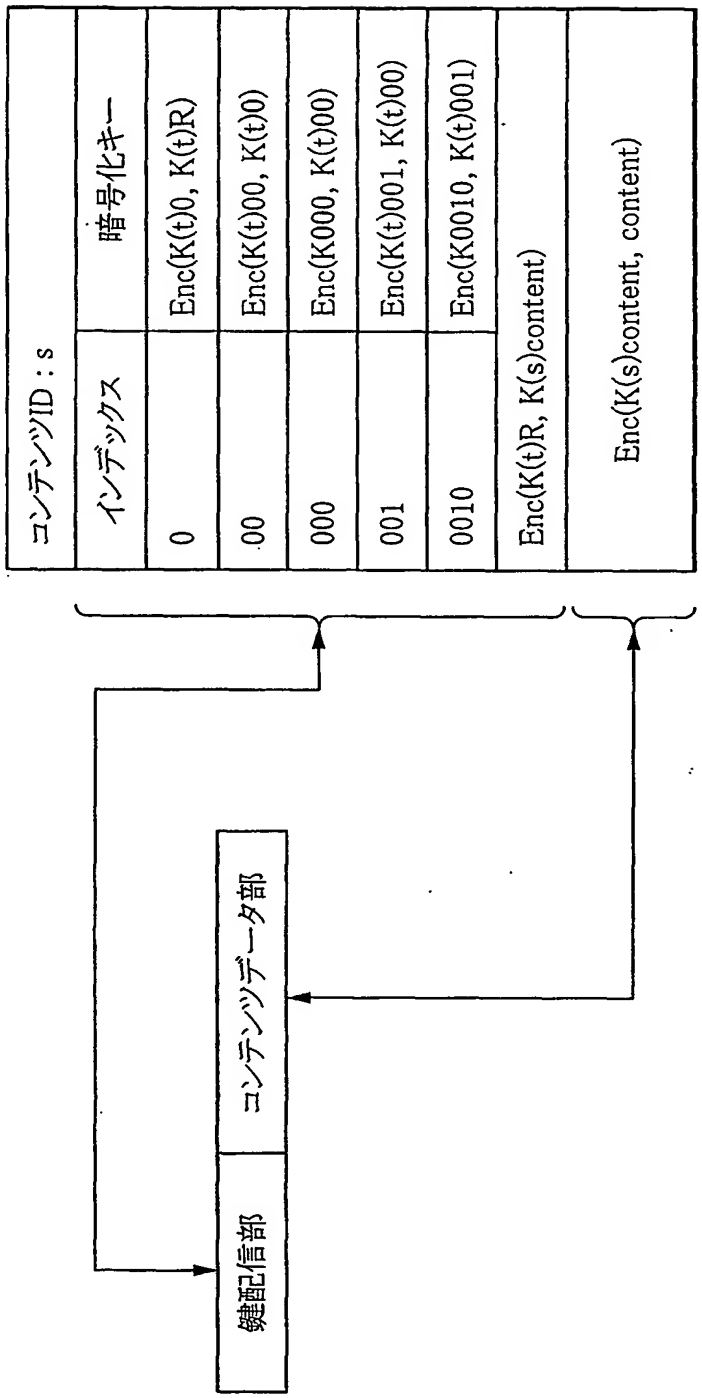

鍵配信部
コンテンツデータ部
コンテンツID：s
インデックス
暗号化キー
0
Enc(K(t)0, K(t)R)
00
Enc(K(t)00, K(t)0)
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)R, K(s)content)
Enc(K(s)content, content)

FIG.20

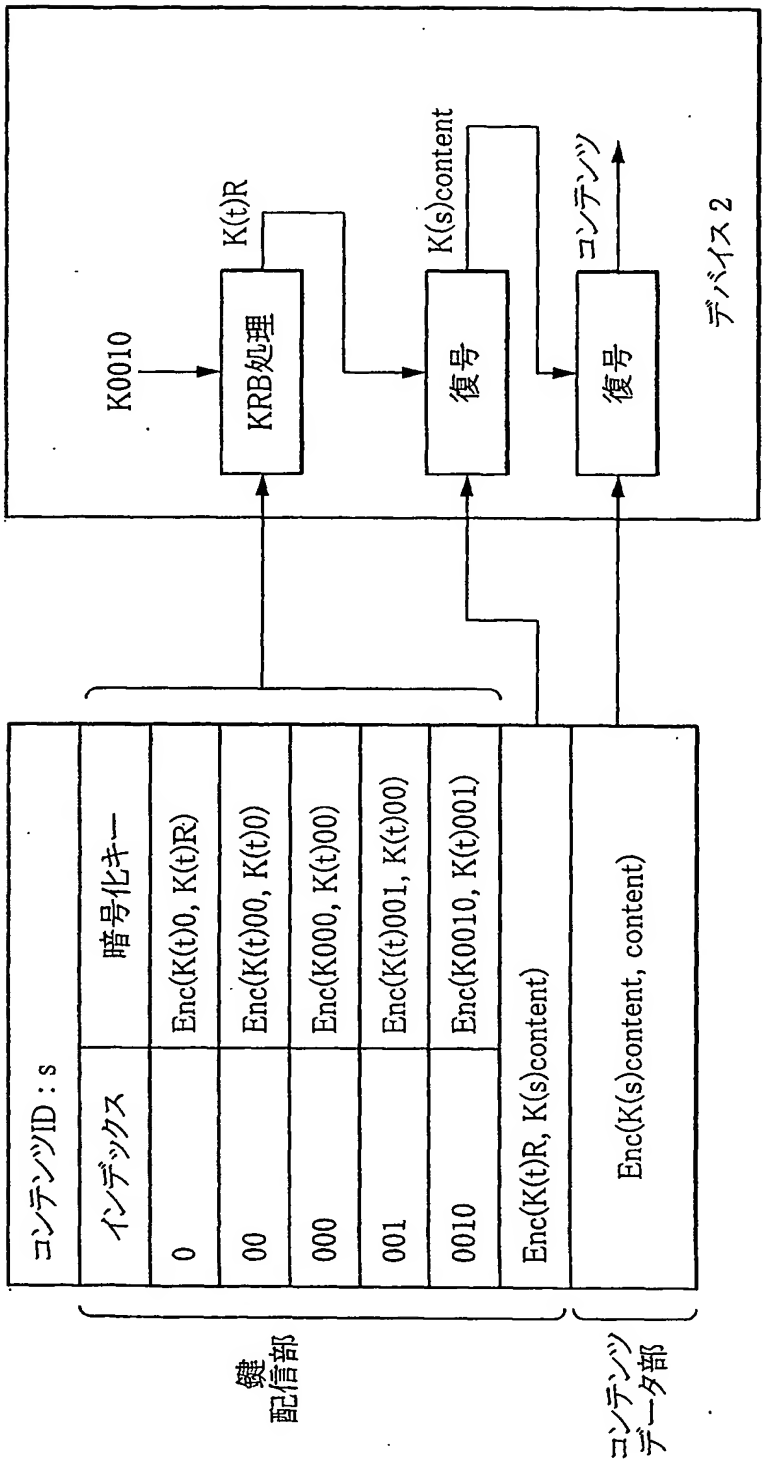

K0010
KRB処理
K(t)R
復号
K(s)content
復号
コンテンツ
デバイス 2
コンテンツID：s
インデックス
暗号化キー
0
Enc(K(t)0, K(t)R)
00
Enc(K(t)00, K(t)0)
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)R, K(s)content)
Enc(K(s)content, content)
鍵配信部
コンテンツデータ部

FIG.21

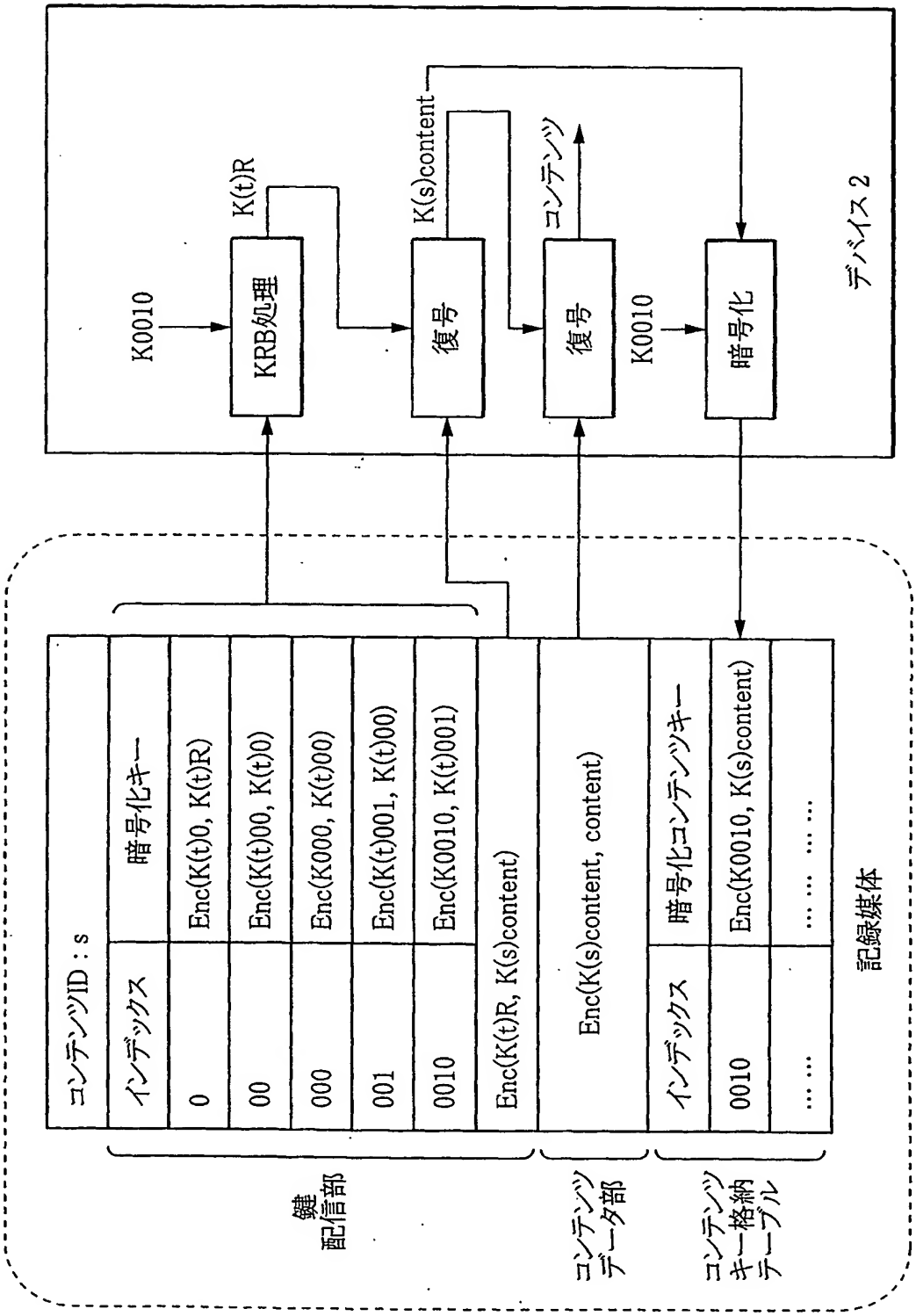

デバイス 2
K0010
KRB処理
K(t)R
復号
K(s)content
復号
コンテンツ
K0010
暗号化
記録媒体
コンテンツID：s
インデックス
暗号化キー
0
Enc(K(t)0, K(t)R)
00
Enc(K(t)00, K(t)0)
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)R, K(s)content)
Enc(K(s)content, content)
インデックス
暗号化コンテンツキー
0010
Enc(K0010, K(s)content)
鍵配信部
コンテンツデータ部
コンテンツキー格納テーブル

FIG.22

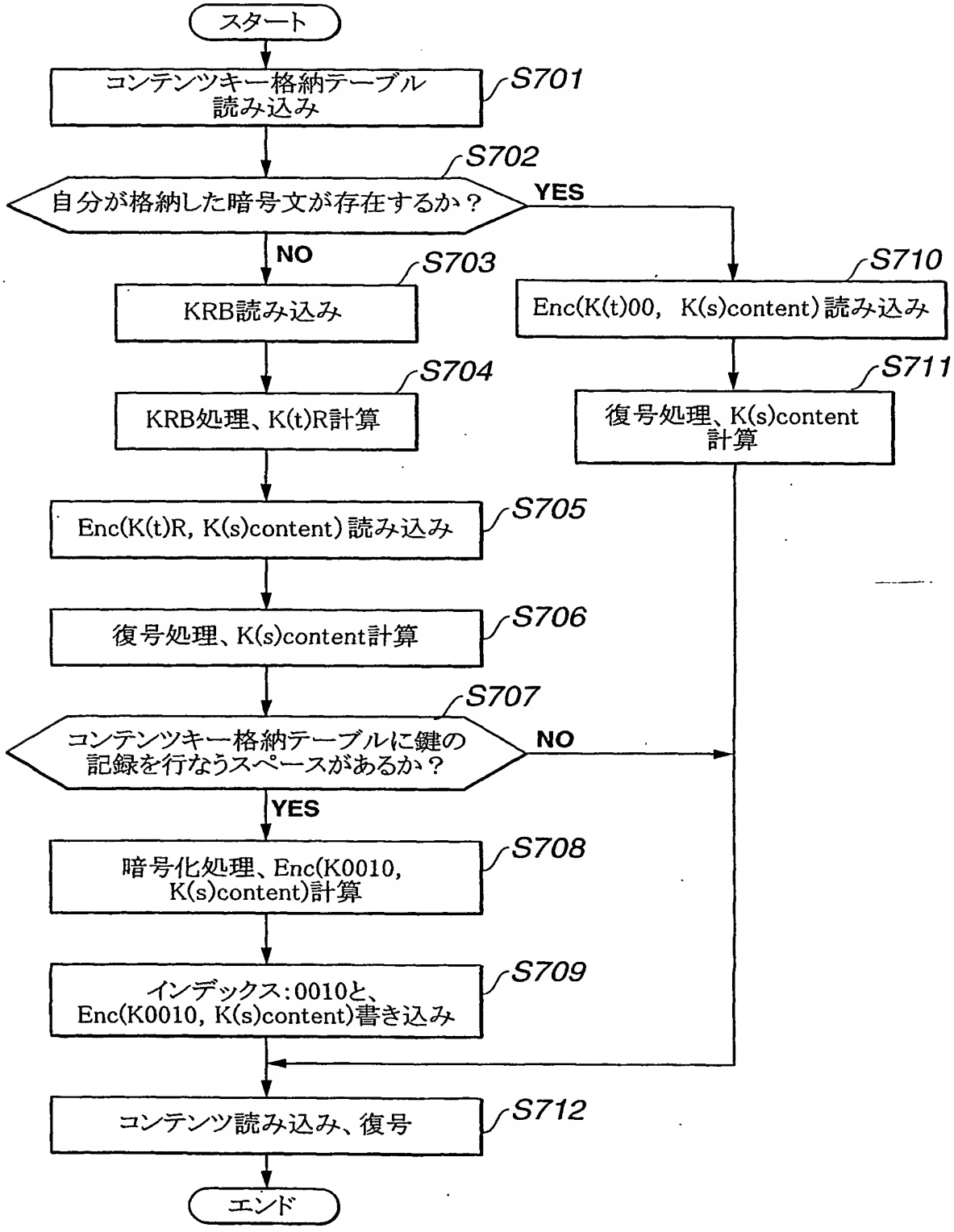

スタート
コンテンツキー格納テーブル読み込み
S701
S702
自分が格納した暗号文が存在するか？
YES
NO
S703
KRB読み込み
S704
KRB処理、K(t)R計算
Enc(K(t)R, K(s)content)読み込み
S705
復号処理、K(s)content計算
S706
S707
コンテンツキー格納テーブルに鍵の記録を行なうスペースがあるか？
NO
YES
暗号化処理、Enc(K0010, K(s)content)計算
S708
インデックス:0010と、Enc(K0010, K(s)content)書き込み
S709
S710
Enc(K(t)00, K(s)content)読み込み
S711
復号処理、K(s)content計算
コンテンツ読み込み、復号
S712
エンド

FIG.23

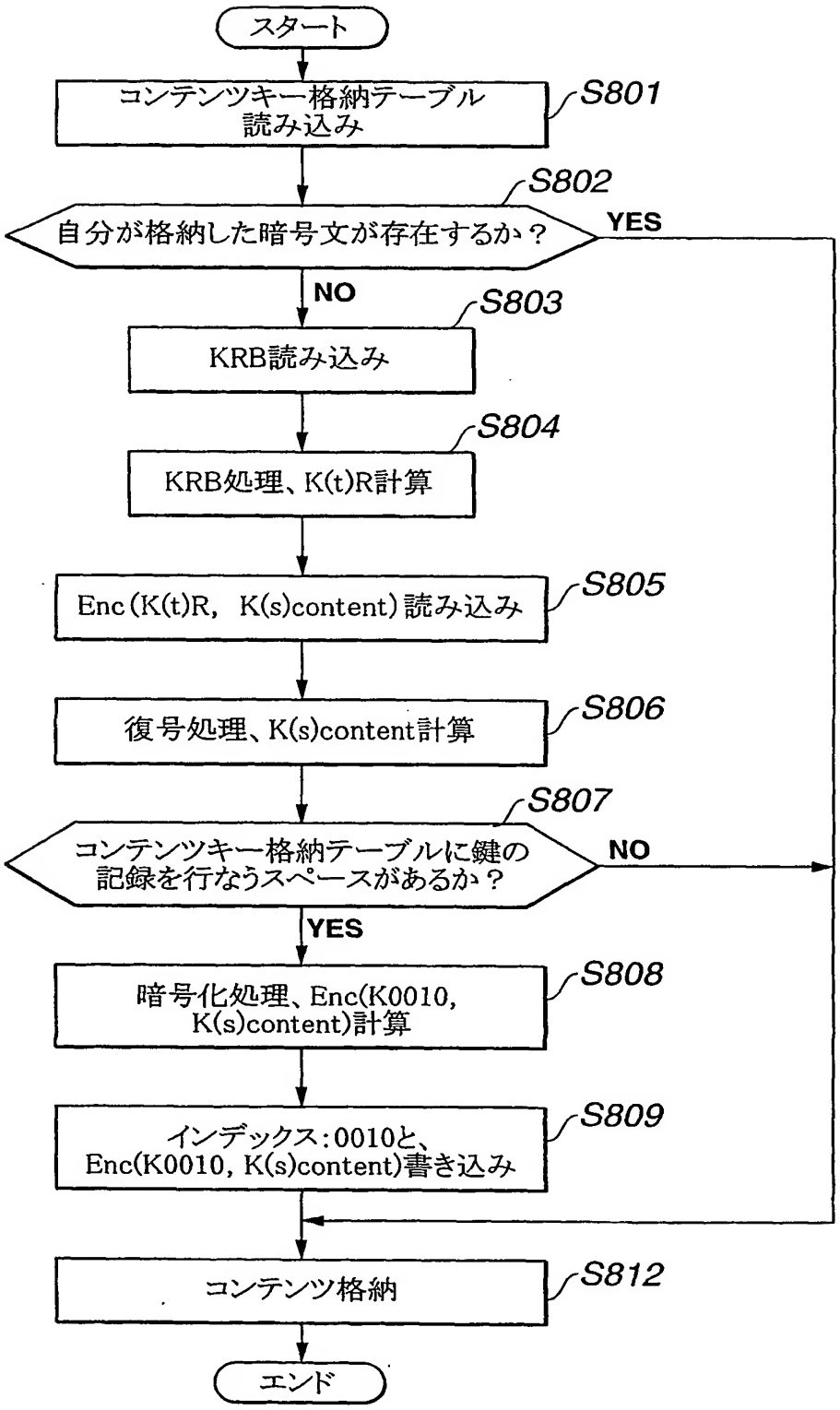

スタート
コンテンツキー格納テーブル
読み込み
S801
S802
自分が格納した暗号文が存在するか？
YES
NO
S803
KRB読み込み
S804
KRB処理、K(t)R計算
Enc(K(t)R, K(s)content)読み込み
S805
復号処理、K(s)content計算
S806
S807
コンテンツキー格納テーブルに鍵の
記録を行なうスペースがあるか？
NO
YES
暗号化処理、Enc(K0010,
K(s)content)計算
S808
インデックス:0010と、
Enc(K0010, K(s)content)書き込み
S809
コンテンツ格納
S812
エンド

FIG.24

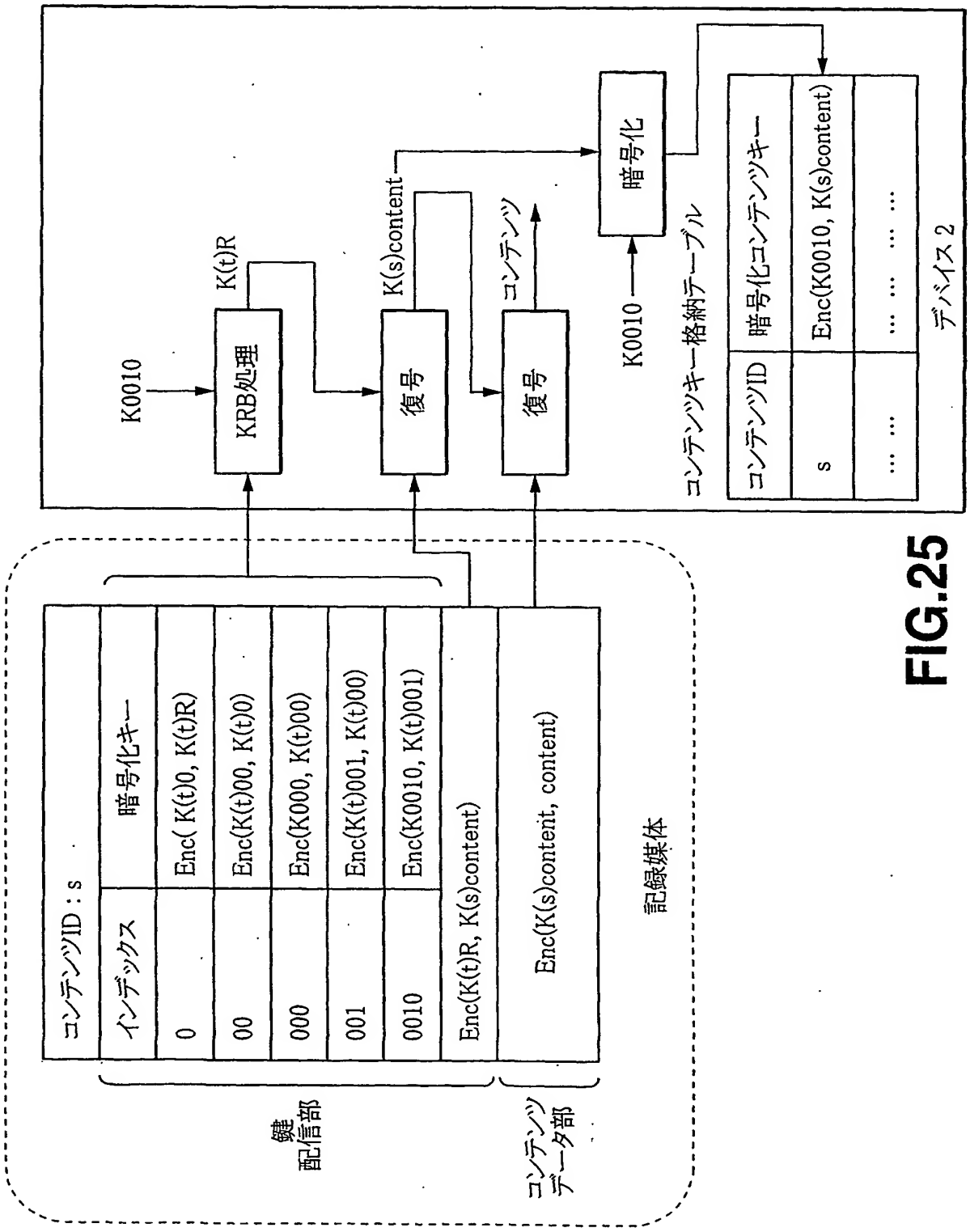

K0010
KRB処理
K(t)R
復号
K(s)content
復号
コンテンツ
暗号化
K0010
コンテンツキー格納テーブル
コンテンツID
暗号化コンテンツキー
s
Enc(K0010, K(s)content)
デバイス2
コンテンツID：s
インデックス
暗号化キー
0
Enc(K(t)0, K(t)R)
00
Enc(K(t)00, K(t)0)
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)R, K(s)content)
Enc(K(s)content, content)
記録媒体
鍵配信部
コンテンツデータ部

FIG.25

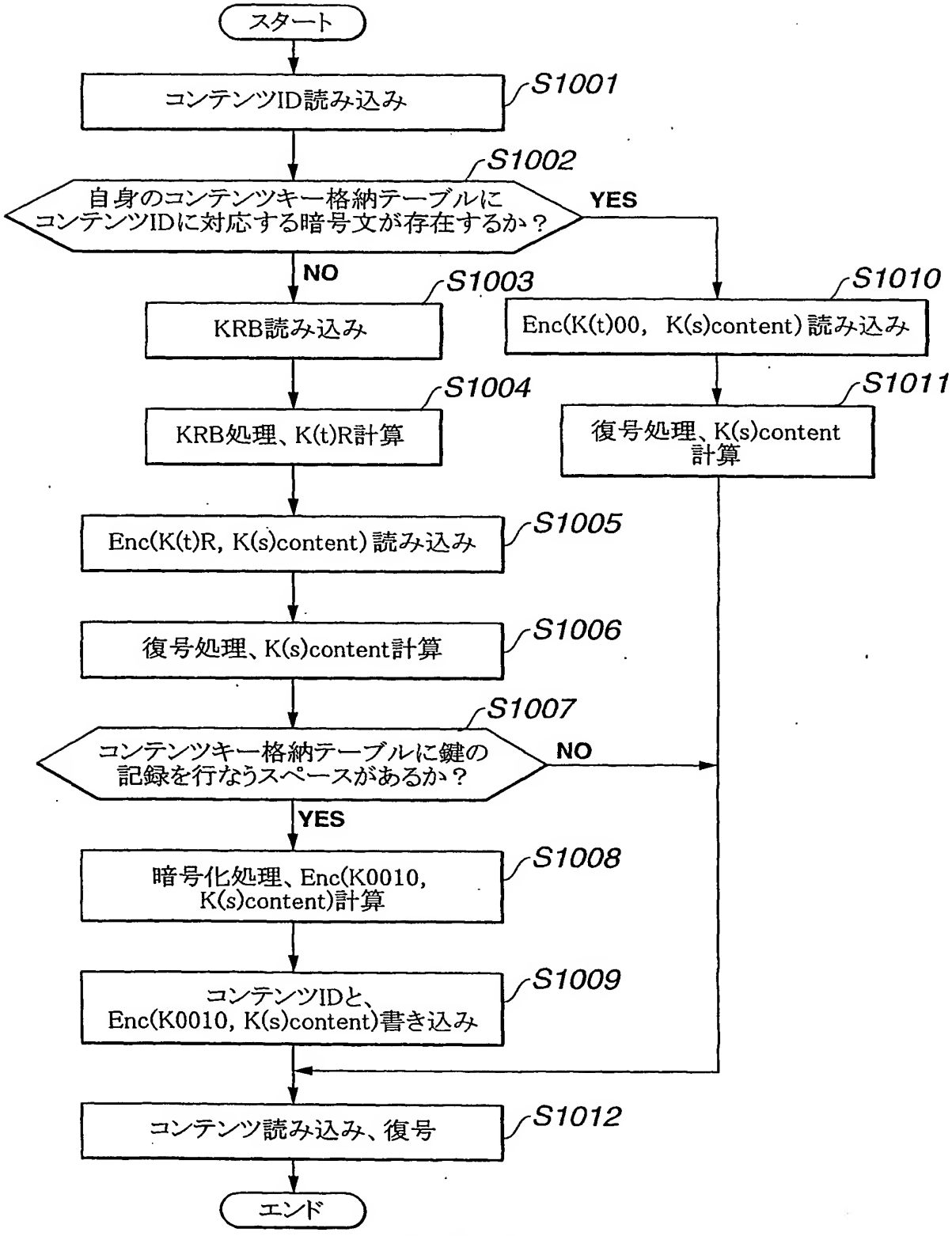

スタート
コンテンツID読み込み
S1001
S1002
自身のコンテンツキー格納テーブルに
コンテンツIDに対応する暗号文が存在するか？
YES
NO
S1003
KRB読み込み
S1004
KRB処理、K(t)R計算
S1005
Enc(K(t)R, K(s)content) 読み込み
S1006
復号処理、K(s)content計算
S1007
コンテンツキー格納テーブルに鍵の
記録を行なうスペースがあるか？
NO
YES
S1008
暗号化処理、Enc(K0010,
K(s)content)計算
S1009
コンテンツIDと、
Enc(K0010, K(s)content)書き込み
S1010
Enc(K(t)00, K(s)content) 読み込み
S1011
復号処理、K(s)content
計算
S1012
コンテンツ読み込み、復号
エンド

FIG.26

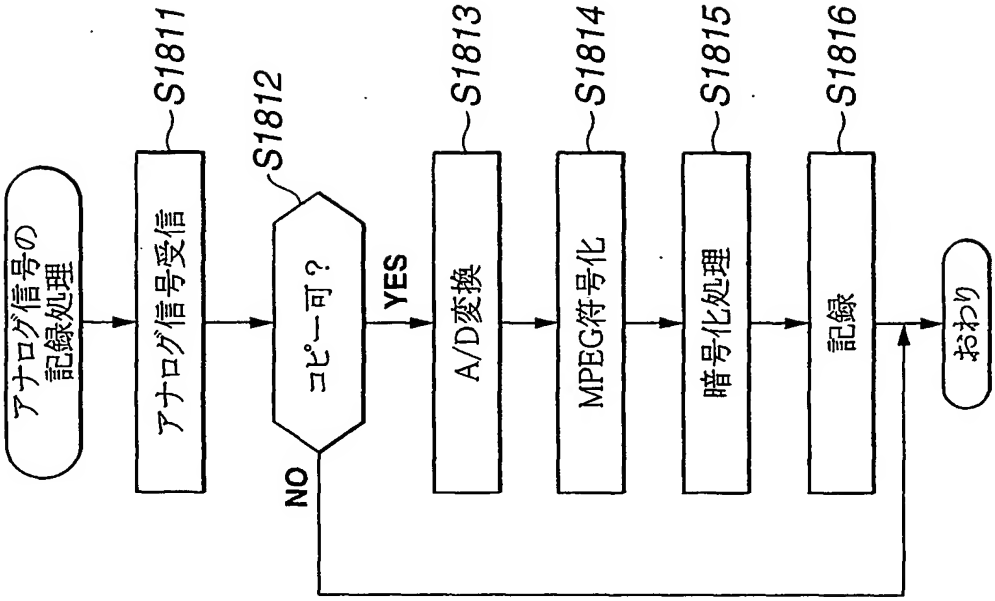


FIG.27B

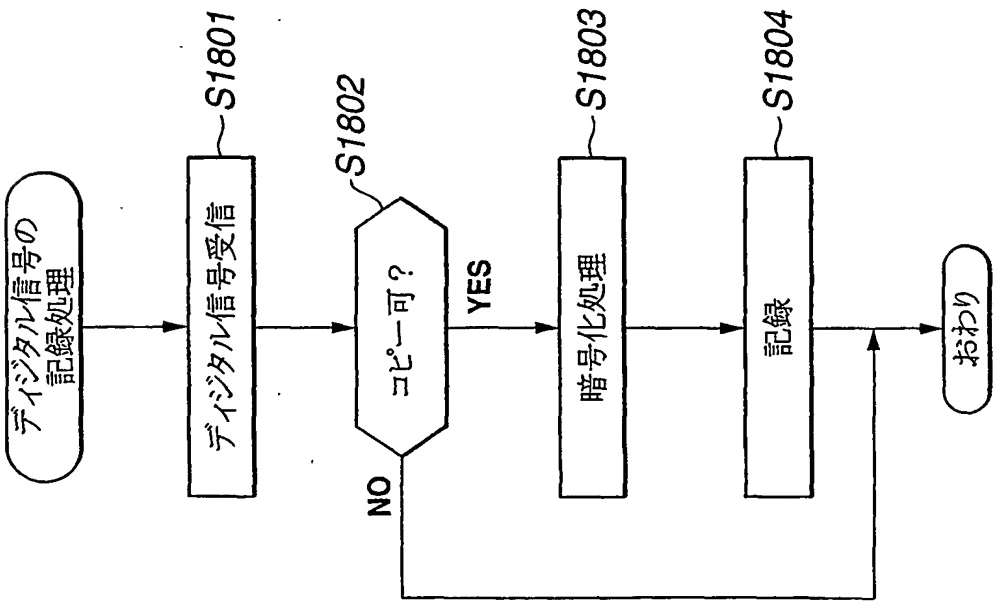


FIG.27A

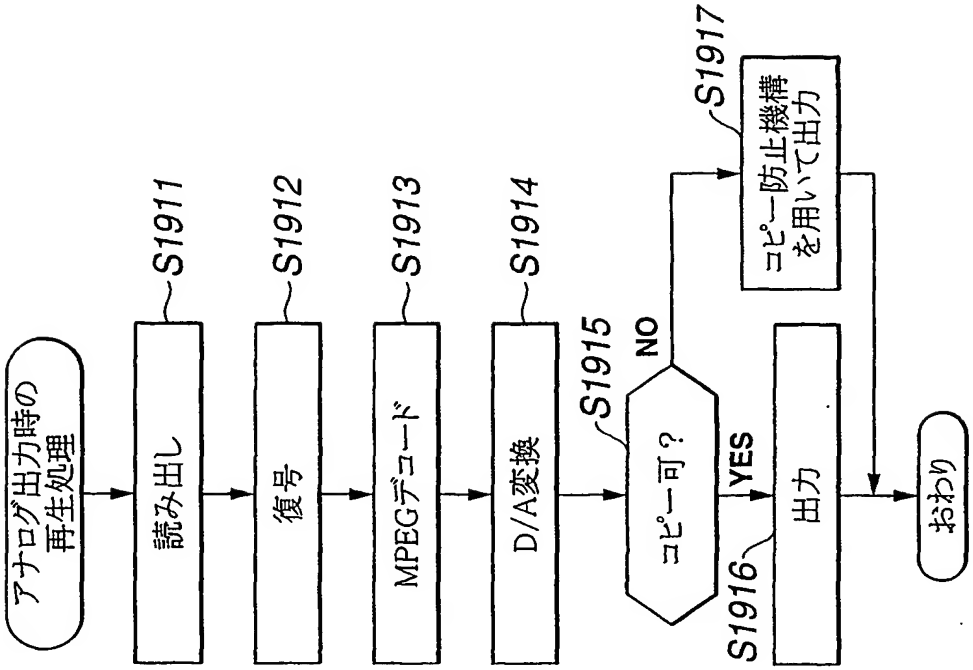


FIG.28B

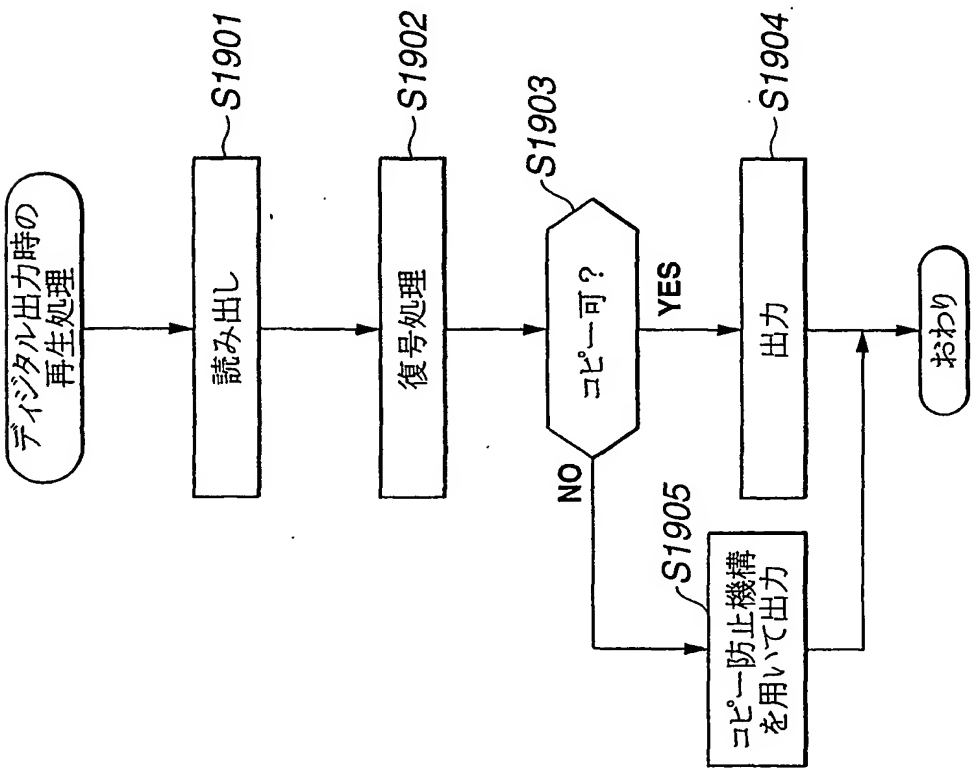


FIG.28A

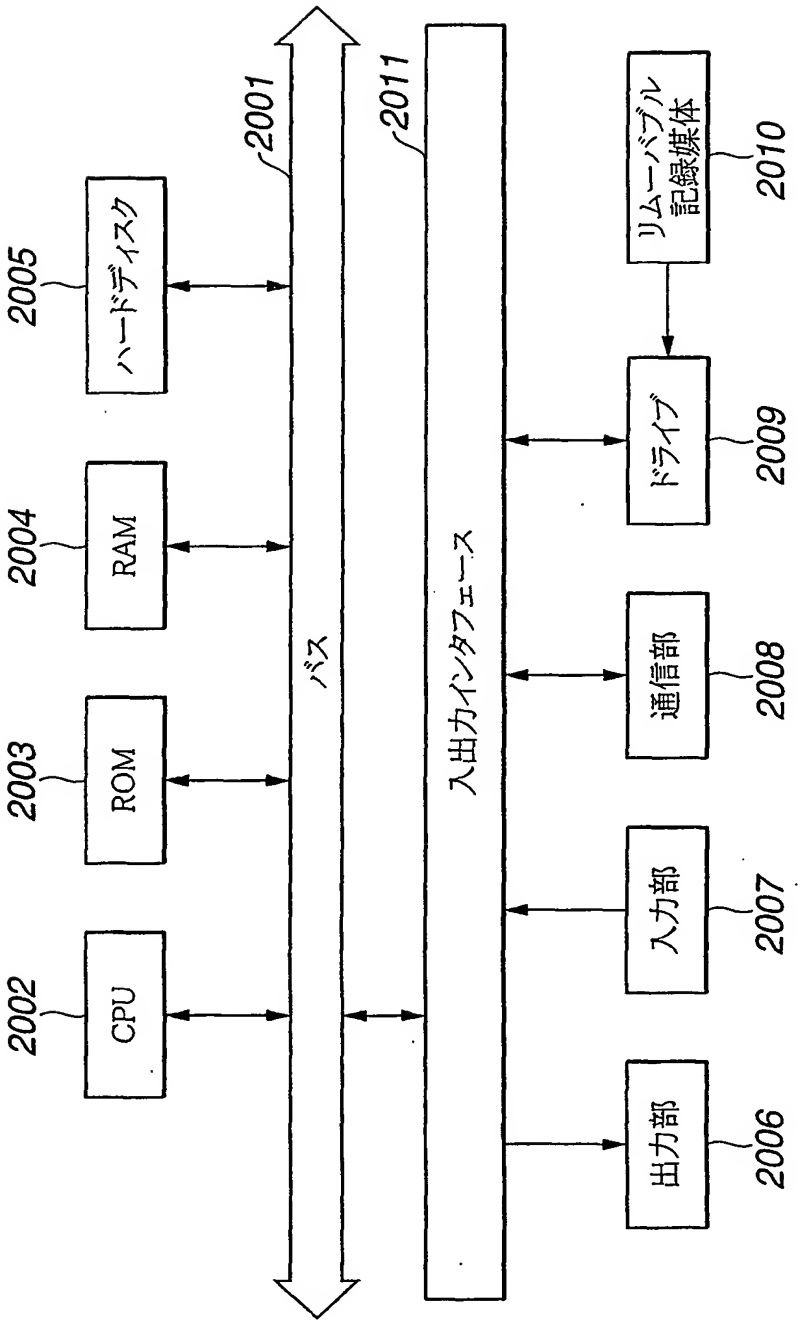

2001
2011
2005
ハードディスク
2004
RAM
2003
ROM
2002
CPU
バス
入出力インタフェース
リムーバブル記録媒体
2010
ドライブ
2009
通信部
2008
入力部
2007
出力部
2006

FIG.29

国際調査報告

国際出願番号 PCT／JP01／05327

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G11B20／10, G10K15／02, G06F12／14

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G11B20／10, G10K15／02, G06F12／14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース key, tree, generation, DVD

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management.	10, 24, 30
Y	IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol.17, No.9 , p.1614-1631, especially pp.1616-1621	1- 9, 11, 15-23, 25, 29, 31
A		12-14, 26-28, 32
Y	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワークの安全性, 日本経済新聞社, 29.7月.1983(29.07.83), p.201-206 (特にp.204 3データ暗号鍵の登録 を参照)	1- 9, 15-23, 29

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 07.09.01	国際調査報告の発送日 18.09.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 印 5M 9364 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT／JP01／05327

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	EP 969667 A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 5.1月.2000(05.01.00), 第33-39段落 & JP 2000-23137 A, 第61, 66, 67段落 & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11, 25, 31
Y	JP 9-115241 A (ソニー株式会社) 2.5月.1997(02.05.97), 第21, 22, 28段落 & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (ソニー株式会社) 30.11月.1999(30.11.99), 第16, 18, 19, 57, 58段落 & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	1-32
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98 ,1998 ,p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-33

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０５３２７

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の５群の発明に区分される。

1．請求の範囲1-9, 15-23, 29
2．請求の範囲10, 24, 30
3．請求の範囲11, 25, 31
4．請求の範囲12-14, 26-28, 32
5．請求の範囲33

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

INTERNATION SEARCH REPORT

Int nal application No.
PCT/JP01/05327

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/00, G11B20/10, G10K15/02, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00, G11B20/10, G10K15/02, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST FILE on Science and Technology key, tree, generation, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WALDVOGEL, M. et al., "The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, September, 1999, Vol.17, No.9, pages 1614 to 1631, especially pages 1616 to 1621	10,24,30 1-9,11,15-23, 25,29,31
A		12-14,26-28,32
Y	supervised by Shin ICHIMATSU, "Data Hogo to Angou-ka no Kenkyu; Computer Network no Anzensei", Nippon Keizai Shinbunsha, 29 July, 1983 (29.07.83), pages 201 to 206, (especially, page 204, 3 Data Angou Kagi no Touroku)	1-9,15-23,29
Y	EP 969667 A2 (Matsushita Electric Industrial Co., Ltd.), 05 January, 2000 (05.01.00), Par. Nos. [0033] to [0039] & JP 2000-23137 A Par. Nos. [0061], [0066], [0067] & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11,25,31

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 September, 2001 (07.09.01)	18 September, 2001 (18.09.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATI(L SEARCH REPORT

national application No.
PCT/JP01/05327

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-115241 A (Sony Corporation), 02 May, 1997 (02.05.97), Par. Nos. [0021], [0022], [0028] & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (Sony Corporation), 30 November, 1999 (30.11.99), Par. Nos. [0016], [0018], [0019], [0057], [0058] & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (IBM Japan, Ltd.), 09 July, 1999 (09.07.99), Par. Nos. [0009] to [0011], [0017] to [0022] & CN 1224962 A	1-32
A	WONG, C. K. et al., "Secure Group Communications Using Key Graphs", In: Proceedings of ACM SIGCOMM'98, (1998), pages 68 to 79, especially, 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
PA	Makoto TATEBAYASHI et al., "Kiroku Media no Contents Hogo System", 2000 nen Denshi Joho Tsuushin Gakkai Kiso Kyoukai Society Taikai Kouen Ronbunshuu, 07 September, 2000 (07.09.00), pages 367 to 368	1-33

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05327

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This applied invention is classified into the following five groups of inventions:

1. Claims 1-9, 15-23, 29,
2. Claims 10, 24, 30,
3. Claims 11, 25, 31,
4. Claims 12-14, 26-28, 32, and
5. Claim 33.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

特　許　協　力　条　約

EP ・ US　　PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　ＳＫ０１ＰＣＴ８７	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０１／０５３２７	国際出願日 （日.月.年）　２１．０６．０１	優先日 （日.月.年）　２１．０６．００
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☒ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　１２　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP01／05327

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の５群の発明に区分される。

1．請求の範囲1-9, 15-23, 29
2．請求の範囲10, 24, 30
3．請求の範囲11, 25, 31
4．請求の範囲12-14, 26-28, 32
5．請求の範囲33

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP01／05327

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G10K15／02, G06F12／14

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G10K15／02, G06F12／14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース　key, tree, generation, DVD

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management.	10, 24, 30
Y	IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol.17, No.9 , p.1614-1631, especially pp.1616-1621	1- 9, 11, 15-23, 25, 29, 31
A		12-14, 26-28, 32
Y	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワークの安全性, 日本経済新聞社, 29.7月.1983(29.07.83), p.201-206 （特にp.204 3データ暗号鍵の登録 を参照）	1- 9, 15-23, 29

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　07. 09. 01	国際調査報告の発送日　18.09.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　中里　裕正　5M　9364 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	EP 969667 A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 5.1月.2000(05.01.00), 第33-39段落 & JP 2000-23137 A, 第61, 66, 67段落 & AU 9937949 A & SG 71930 A & CN 124961 A & KR 2000011441 A & TW 416246 A	11, 25, 31
Y	JP 9-115241 A (ソニー株式会社) 2.5月.1997(02.05.97), 第21, 22, 28段落 & EP 751516 A2 & KR 97002629 & US 6134201 A & US 6215745 B1	33
Y	JP 11-328850 A (ソニー株式会社) 30.11月.1999(30.11.99), 第16, 18, 19, 57, 58段落 & EP 996074 A1 & WO 99/59092 A & CN 1273657 A	33
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	1-32
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98 ,1998 ,p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-32
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-33